MES-2110

Intelligent Layer 2 Switch

User's Guide

Default Login Details

IP Address	http://192.168.1.1
User Name	admin
Password	1234

Firmware Version 1.00
Edition 4, 05/2010

ZyXEL

www.zyxel.com

Copyright © 2010
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the MES-2110 using the web configurator.

Related Documentation

- Command Line Interface (CLI) Reference Guide

  Line commands offer an alternative to the web configurator and in some cases are necessary to configure advanced features.

Note: It is recommended you use the web configurator to configure the MES-2110.

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.

- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

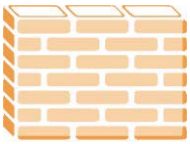
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The MES-2110 may be referred to as the "MES-2110", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The MES-2110 icon is not an exact representation of your device.

The MES-2110	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Router	

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Do not obstruct the device ventillation slots as insufficient airflow may harm your device.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Use ONLY power wires of the appropriate wire gauge (see Chapter 25 on page 215 for details) for your device. Connect it to a power supply of the correct voltage (see Chapter 25 on page 215 for details).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- The length of exposed (bare) power wire should not exceed 7 mm.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

Introduction 19
Hardware Installation and Connection 25
Hardware Overview 29
Tutorials 37
The Web Configurator 51
System Details 61
Configuration 65
Loop Detection 71
Jumbo Frame 75
802.1x 77
Bridge 89
VLAN 97
Bandwidth Control 111
Broadcast Storm Control 113
Port Mirroring 115
Link Aggregation 117
IGMP 123
DHCP Relay Configuration 137
IP Source Guard 141
MAC 151
QoS 157
Mgmt Config and System Restart Menu 165
Command Line Interface 179
Troubleshooting 207
Product Specifications 215

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Contents Overview 9

Table of Contents 11

Chapter 1
Introduction 19

1.1 Overview 19
1.1.1 Backbone Application 19
1.1.2 Bridging Example 20
1.1.3 High Performance Switching Example 21
1.1.4 IEEE 802.1Q VLAN Application Examples 21
1.1.5 Metro Ethernet 22
1.2 Ways to Manage the MES-2110 23
1.3 Good Habits for Managing the MES-2110 24

Chapter 2
Hardware Installation and Connection 25

2.1 Installation Scenarios 25
2.2 Desktop Installation Procedure 25
2.3 Mounting the MES-2110 on a Rack 26
2.3.1 Rack-mounted Installation Requirements 26
2.3.2 Attaching the Mounting Brackets to the MES-2110 27
2.3.3 Mounting the MES-2110 on a Rack 28

Chapter 3
Hardware Overview 29

3.1 Front Panel 29
3.1.1 Console Port 30
3.1.2 Gigabit Ethernet Ports 30
3.1.3 Mini-GBIC Slots 31
3.2 AC Power Connection 33
3.3 DC Power Connection 34
3.4 LEDs 35

Chapter 4
Tutorials 37

4.1 IGMP Snooping 37
4.2 RADIUS Configuration 38
4.3 MVR Configuration 41
4.4 VLAN ID Priority 44
4.5 Untrusted ARP Inspection 45
4.6 Outgoing Traffic Bandwidth 47
4.7 Frame Tagging 48

Chapter 5
The Web Configurator 51

5.1 Introduction 51
5.2 System Login 51
5.3 The Main Screen 53
5.3.1 Set Up the Administrative Password 58
5.4 Saving Your Configuration 58
5.5 Switch Lockout 59
5.6 Resetting the MES-2110 59
5.6.1 Reload the Configuration File 59

Chapter 6
System Details 61

6.1 Overview 61
6.2 The System Information Screen 61
6.3 The Board Information Screen 62
6.4 The DHCP Configuration Screen 63

Chapter 7
Configuration 65

7.1 Overview 65
7.2 The Port Configuration Screen 65
7.3 The Port Status Screen 67
7.4 The RMON Status Screen 68

Chapter 8
Loop Detection 71

8.1 Overview 71
8.2 The Loop Detection Screen 72

Chapter 9
Jumbo Frame 75

9.1 Overview 75

9.2 The Jumbo Frame Configuration Screen 75

Chapter 10
802.1x 77

10.1 Overview 77
10.1.1 IEEE 802.1x Authentication 77
10.1.2 Guest VLAN 78
10.2 802.1x Global Configuration Screen 79
10.3 802.1x Radius Server Configuration Screen 80
10.4 802.1x Port Configuration Screen 81
10.5 802.1x Radius Server Configuration Screen 83
10.6 Technical Reference 84
10.6.1 RADIUS and TACACS+ 84
10.6.2 Supported RADIUS Attributes 84
10.6.3 Attributes Used for Authentication 85
10.6.4 Attributes Used for Accounting 86

Chapter 11
Bridge 89

11.1 Overview 89
11.1.1 STP Terminology 89
11.1.2 How STP Works 90
11.1.3 STP Port States 91
11.2 The Bridge Configuration Screen 91
11.3 The RSTP System Configuration Screen 92
11.4 The Spanning Tree Port Configuration 95

Chapter 12
VLAN 97

12.1 Overview 97
12.2 Introduction to IEEE 802.1Q Tagged VLANs 97
12.2.1 Forwarding Tagged and Untagged Frames 98
12.3 The VLAN Type Screen 99
12.4 The Port-Based VLAN Screen 99
12.5 The Tag-Based VLAN Screens 101
12.5.1 VLAN Stacking 101
12.5.2 VLAN Stacking Example 101
12.5.3 VLAN Stacking Port Roles 102
12.5.4 VLAN Tag Format 103
12.5.5 Frame Format 104
12.5.6 The VLAN Stacking Configuration Screen 105
12.5.7 The Tag-Based Port Information Screen 107
12.5.8 The Tag-Based Port Configuration Screen 108

12.5.9 The Management VLAN Screen 109

Chapter 13
Bandwidth Control 111

13.1 Overview 111
13.2 Bandwidth Control Setup 111

Chapter 14
Broadcast Storm Control 113

14.1 Overview 113
14.2 Broadcast Storm Control Setup 113

Chapter 15
Port Mirroring 115

15.1 Overview 115
15.2 Port Mirroring Setup 115

Chapter 16
Link Aggregation 117

16.1 Overview 117
16.2 Dynamic Link Aggregation 117
16.2.1 Link Aggregation ID 118
16.3 Static Trunking Example 118
16.4 Link Aggregation Setting 119
16.5 Link Aggregation Control Protocol 120
16.6 LACP Link Status 121

Chapter 17
IGMP 123

17.1 Overview 123
17.1.1 IP Multicast Addresses 123
17.1.2 IGMP Snooping 123
17.1.3 IGMP Snooping and VLANs 124
17.2 IGMP Configuration 124
17.2.1 IGMP VLAN Query Mode 126
17.3 IGMP Status 127
17.4 MVR Overview 127
17.4.1 Types of MVR Ports 128
17.4.2 MVR Modes 128
17.4.3 How MVR Works 128
17.5 General MVR Configuration 129
17.6 MVR Group Configuration 131
17.6.1 MVR Configuration Example 133

Chapter 18
DHCP Relay Configuration 137

18.1 Overview 137
18.1.1 DHCP Relay Agent Information 137
18.2 DHCP Relay Configuration 138

Chapter 19
IP Source Guard 141

19.1 Overview 141
19.1.1 DHCP Snooping Overview 142
19.2 DHCP Snooping Configuration 143
19.3 DHCP Binding Table 145
19.4 The ARP Inspection Screen 147
19.4.1 Configuring ARP Inspection 147

Chapter 20
MAC 151

20.1 Overview 151
20.2 The MAC Table Status Screen 152
20.3 The Lock MAC Address Learning Screen 153
20.4 The MAC Filter Configuration Screen 154
20.5 The MAC Limit Configuration Screen 156

Chapter 21
QoS 157

21.1 Overview 157
21.2 The QoS Base Configuration Screen 157
21.2.1 Configuring the Base Configuration Screen 158
21.3 The 802.1p Priority Table 160
21.4 The Tag Priority Table 161
21.5 The IP DSCP Priority Table 161
21.6 The Priority Override Configuration Screen 163

Chapter 22
Mgmt Config and System Restart Menu 165

22.1 Overview 165
22.2 The Serial Port Configuration Screen 165
22.3 The SNMP Configuration Screens 166
22.3.1 The SNMP Communities Screen 167
22.3.2 The IP Trap Manager Screen 167
22.4 The SNTP Screen 168
22.5 Alarms and Logs 170
22.6 The User Configuration Screen 172

22.7 The Cable Test Screen 173
22.8 The Host DoS Protection 174
22.9 The Port Abnormal Traffic Detection Screen 175
22.10 Upgrading the Firmware 176
22.11 Managing the Configuration File 177
22.12 Restarting the System 178

Chapter 23
Command Line Interface 179

23.1 Overview 179
23.1.1 Console Port Management 179
23.1.2 Logging in 179
23.1.3 Using Shortcuts and Getting Help 180
23.2 Saving Changes 180
23.3 Logging Out 181
23.4 Command Modes 181
23.5 Basic Commands 182
23.6 Privileged Command Mode 183
23.7 Configuration Mode 186
23.7.1 IGMP Snooping Example 193
23.7.2 RADIUS Configuration Example 194
23.8 MVR Mode 195
23.8.1 MVR Command Example 196
23.9 VLAN Mode 197
23.9.1 VLAN ID Priority Example 198
23.10 Interface Mode 198
23.10.1 Untrusted ARP Inspection Example 203
23.10.2 Outgoing Traffic Bandwidth Limit Example 203
23.10.3 Frame Tagging Examples 204

Chapter 24
Troubleshooting 207

24.1 Power, Hardware Connections, and LEDs 207
24.2 MES-2110 Access and Login 208
24.3 MES-2110 Configuration and Console 211

Chapter 25
Product Specifications 215

Appendix A Changing a Fuse 219

Appendix B Common Services 221

Appendix C Legal Information 225

Index..... 229

1 Introduction

1.1 Overview

This chapter introduces the main features and applications of the MES-2110.

The MES-2110 is a layer-2 standalone Ethernet switch with additional layer-2, layer-3, and layer-4 features suitable for metro ethernets. The MES-2110 has eight 10/100 Mbps Ethernet ports and two mini-GBIC slots. It also has two GbE dual personality interfaces with each interface comprising one mini-GBIC slot and one 10/100/1000 Mbps RJ-45 port, with either port or slot active at a time.

With its built-in Web Configurator, managing and configuring the MES-2110 is easy. In addition, the MES-2110 can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

See Chapter 25 on page 215 for a full list of software features available on the MES-2110.

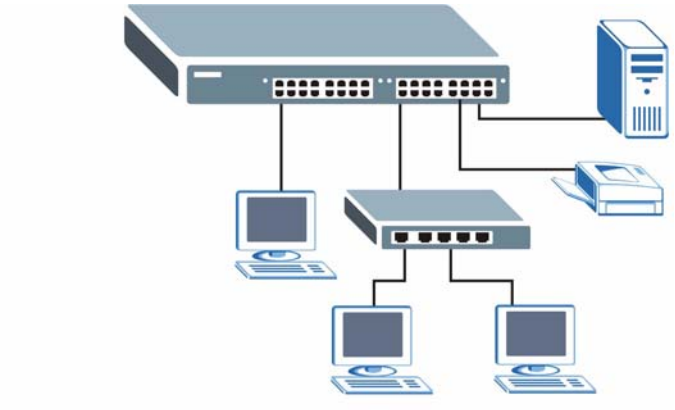
This section shows a few examples of using the MES-2110 in various network environments.

1.1.1 Backbone Application

The MES-2110 is an ideal solution for small networks where rapid growth can be expected in the near future. The MES-2110 can be used standalone for a group of heavy traffic users. You can connect computers and servers directly to the MES-2110's port or connect other switches to the MES-2110.

In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

Figure 1 Backbone Application

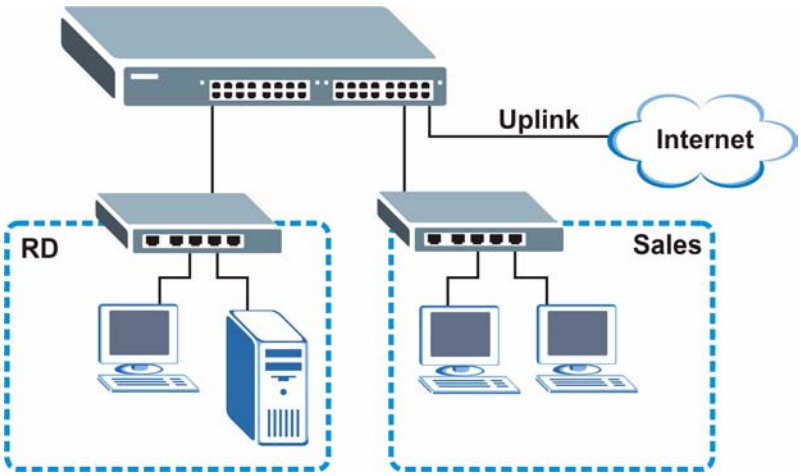


1.1.2 Bridging Example

In this example, the MES-2110 connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the MES-2110. You can provide a super-fast uplink connection by using a Gigabit Ethernet/mini-GBIC port on the MES-2110.

Moreover, the MES-2110 eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 2 Bridging Application

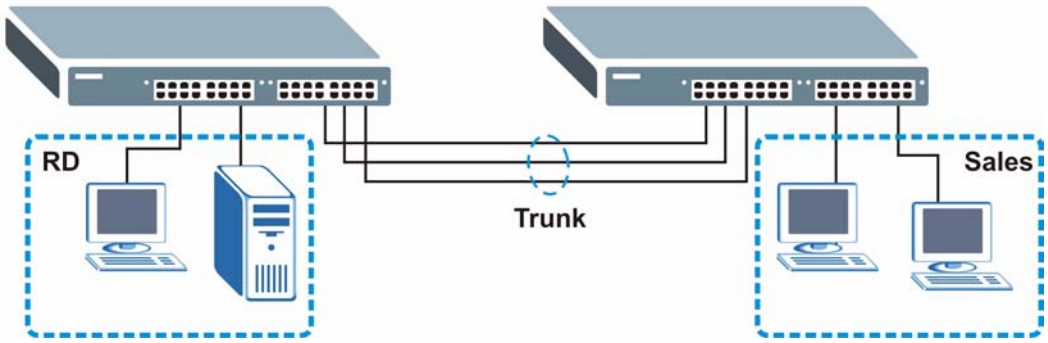


1.1.3 High Performance Switching Example

The MES-2110 is ideal for connecting two networks that need high bandwidth. In the following example, use trunking to connect these two networks.

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The MES-2110 can provide the same bandwidth as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

Figure 3 High Performance Switched Workgroup Application



1.1.4 IEEE 802.1Q VLAN Application Examples

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

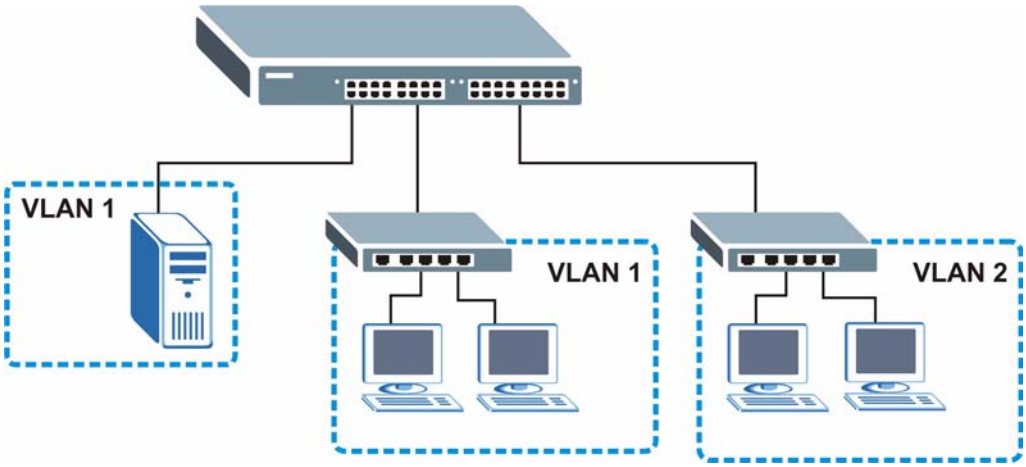
For more information on VLANs, refer to Chapter 12 on page 97.

1.1.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



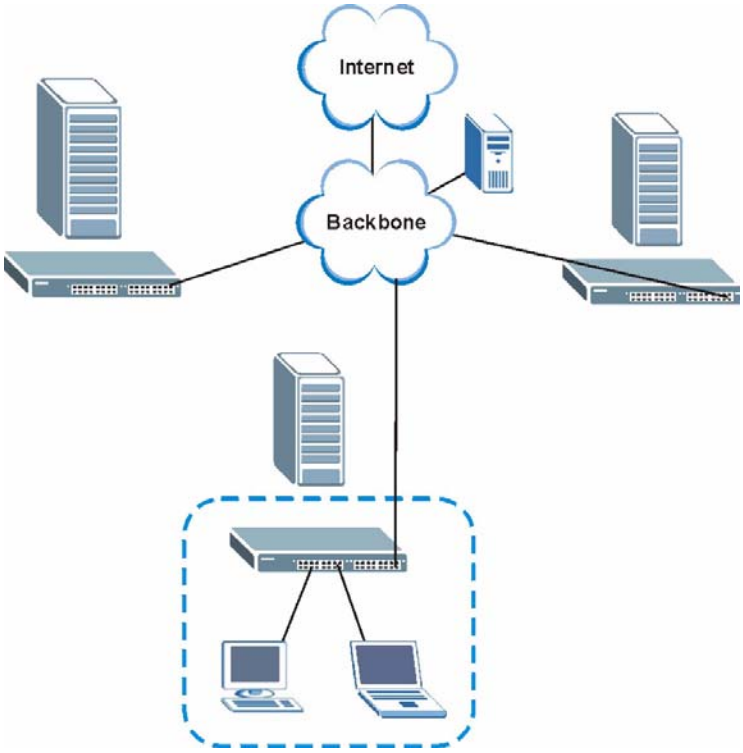
1.1.5 Metro Ethernet

The MES-2110 is ideal for connecting users to an Ethernet network that spans a metropolitan area.

In the following example, the MES-2110 is one of many switches that connect users in the metropolitan area to the Internet. The metro ethernet is based on a star (or hub-and-spoke) topology, though other topologies, such as ring or mesh, are also possible. The MES-2110 is connected to the backbone and the

metropolitan servers over an optical network that provides higher bandwidth than copper.

Figure 5 Metro Ethernet



1.2 Ways to Manage the MES-2110

Use any of the following methods to manage the MES-2110.

- Web Configurator. This is recommended for everyday management of the MES-2110 using a (supported) web browser. See Chapter 5 on page 51.
- Command Line Interface. Line commands offer an alternative to the web configurator and in some cases are necessary to configure advanced features. See the CLI Reference Guide.
- SNMP. The MES-2110 can be monitored by an SNMP manager. See Section 22.3 on page 166.

1.3 Good Habits for Managing the MES-2110

Do the following things regularly to make the MES-2110 more secure and to manage the MES-2110 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the MES-2110 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the MES-2110. You could simply restore your last configuration.

2

Hardware Installation and Connection

2.1 Installation Scenarios

This chapter shows you how to install and connect the MES-2110.

The MES-2110 can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

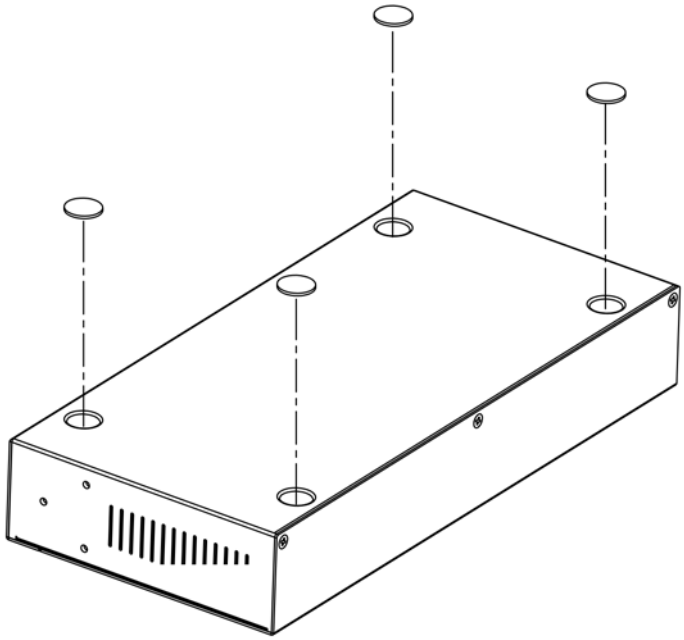
Note: For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the MES-2110. This is especially important for enclosed rack installations.

2.2 Desktop Installation Procedure

1. Make sure the MES-2110 is clean and dry.
2. Set the MES-2110 on a smooth, level surface strong enough to support the weight of the MES-2110 and the connected cables. Make sure there is a power outlet nearby.
3. Make sure there is enough clearance around the MES-2110 to allow air circulation and the attachment of cables and the power cord.
4. Remove the adhesive backing from the rubber feet.

5 Attach the rubber feet to each corner on the bottom of the MES-2110. These rubber feet help protect the MES-2110 from shock or vibration and ensure space between devices when stacking.

Figure 6 Attaching Rubber Feet



Note: Do NOT block the ventilation holes. Leave space between devices when stacking.

2.3 Mounting the MES-2110 on a Rack

The MES-2110 can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your MES-2110 on a standard EIA rack using a rack-mounting kit.

Note: The following sections feature the AC model of the MES-2110 but are equally applicable to the DC model.

2.3.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

Failure to use the proper screws may damage the unit.

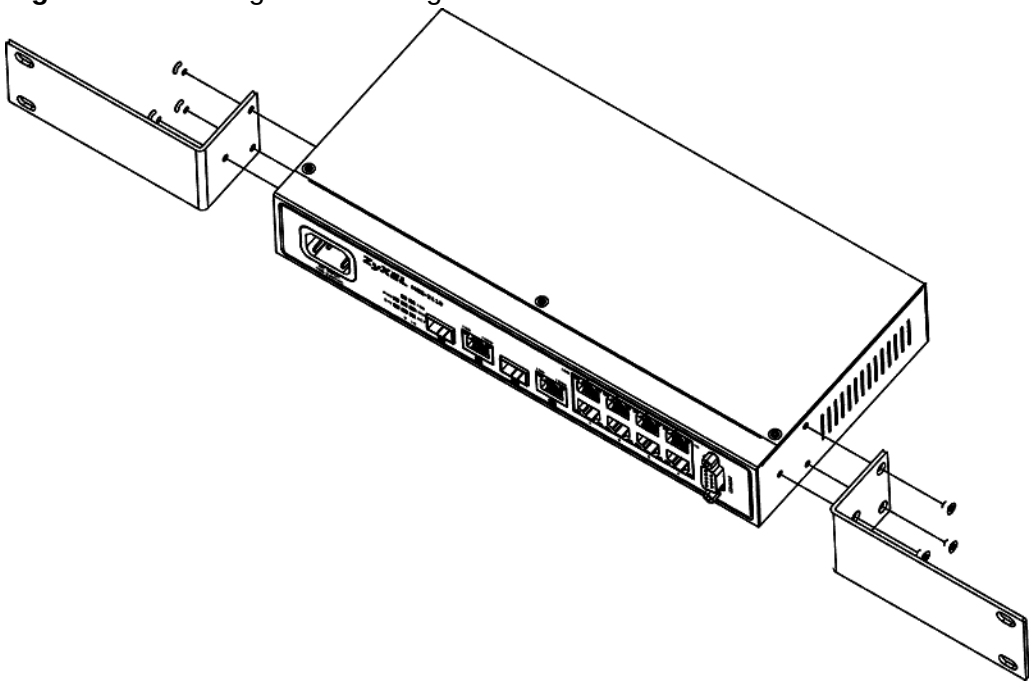
2.3.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the MES-2110 does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.3.2 Attaching the Mounting Brackets to the MES-2110

1 Position a mounting bracket on one side of the MES-2110, lining up the four screw holes on the bracket with the screw holes on the side of the MES-2110.

Figure 7 Attaching the Mounting Brackets



2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the MES-2110.

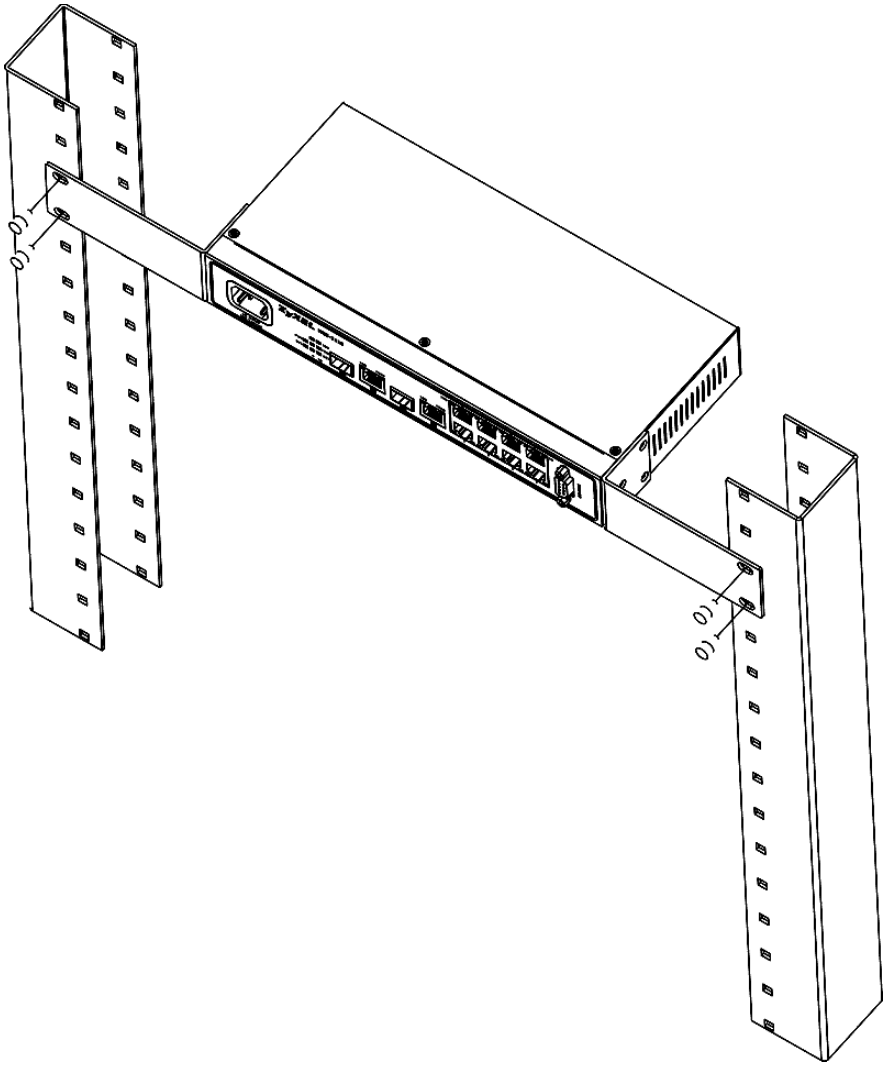
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the MES-2110.

4 You may now mount the MES-2110 on a rack. Proceed to the next section.

2.3.3 Mounting the MES-2110 on a Rack

1 Position a mounting bracket (that is already attached to the MES-2110) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 8 Mounting the MES-2110 on a Rack



2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

3

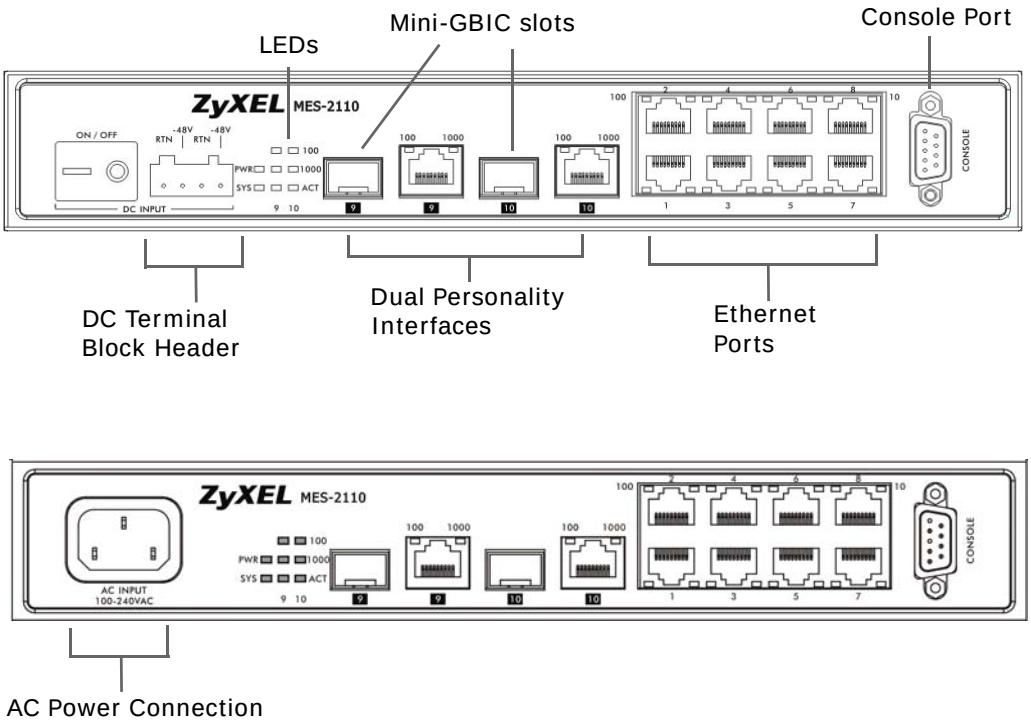
Hardware Overview

This chapter describes the front panel and rear panel of the MES-2110 and shows you how to make the hardware connections.

3.1 Front Panel

The following figure shows the front panel of the MES-2110.

Figure 9 Front Panel



The following table describes the port labels on the front panel.

Table 1 Front Panel Connections

LABEL	DESCRIPTION
Power Connection	Connect an appropriate power supply to this port.
8 10/100 Mbps RJ-45 Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.
Two Mini-GBIC Slots	Use mini-GBIC transceivers in these slots for fiber-optic or copper connections to backbone Ethernet switches.
Two Dual Personality Interfaces	Each interface has one 1000 Base-T copper RJ-45 port and one mini-GBIC slot, with one port active at a time.
	• 10/100/1000 Mbps RJ-45 GbE Ports: Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches.
	• Mini-GBIC Slots: Use mini-GBIC transceivers in these slots for fiber-optic or copper connections to backbone Ethernet switches.
Console Port	The console port is for local configuration of the MES-2110.

3.1.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100
- Terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the MES-2110. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.2 Gigabit Ethernet Ports

The MES-2110 has 1000Base-T auto-negotiating, auto-crossover Ethernet ports. In 10/100/1000 Mbps Fast Ethernet, the speed can be 10 Mbps, 100 Mbps or 1000 Mbps and the duplex mode can be half duplex or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

Two of the 1000Base-T Ethernet ports are paired with a mini-GBIC slot to create a dual personality interface. The MES-2110 uses up to one connection for each mini-GBIC and 1000Base-T Ethernet pair. The mini-GBIC slots have priority over the Gigabit ports. This means that if a mini-GBIC slot and the corresponding GbE port are connected at the same time, the GbE port will be disabled.

When auto-negotiation is turned on, a Ethernet port negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the MES-2110 determines the connection speed by detecting the signal on the cable and using half duplex mode. When the MES-2110's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

3.1.2.1 Default Ethernet Negotiation Settings

The factory default negotiation settings for the Gigabit ports on the MES-2110 are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Link Aggregation: Disabled

3.1.2.2 Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Gigabit port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

3.1.3 Mini-GBIC Slots

These are slots for mini-GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The MES-2110 does not come with transceivers. You must use transceivers that comply with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the MES-2110 is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic or even copper cable connectors.

To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

3.1.3.1 Transceiver Installation

Use the following steps to install a mini-GBIC transceiver (SFP module).

1. Insert the transceiver into the slot with the exposed section of PCB board facing down.
2. Press the transceiver firmly until it clicks into place.
3. The MES-2110 automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.
4. Close the transceiver's latch (latch styles vary).
5. Connect the fiber optic cables to the transceiver.

Figure 10 Transceiver Installation Example

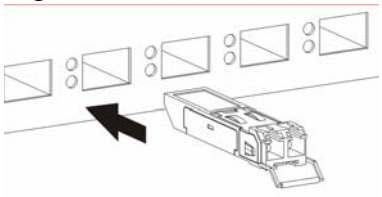
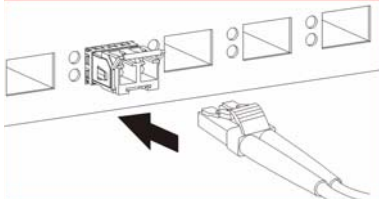


Figure 11 Connecting the Fiber Optic Cables



3.1.3.2 Transceiver Removal

Use the following steps to remove a mini-GBIC transceiver (SFP module).

1. Remove the fiber optic cables from the transceiver.
2. Open the transceiver's latch (latch styles vary).

3 Pull the transceiver out of the slot.

Figure 12 Removing the Fiber Optic Cables

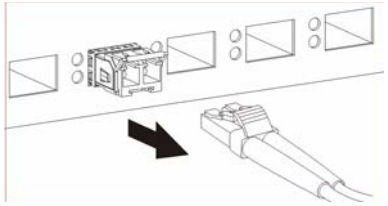


Figure 13 Opening the Transceiver's Latch Example

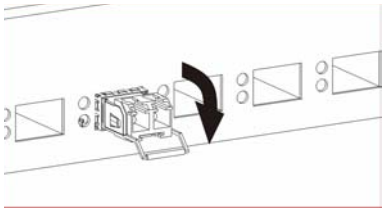
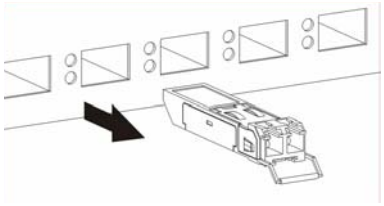


Figure 14 Transceiver Removal Example



3.2 Power Connections Overview

Use the following procedures to connect the MES-2110 to a power source after you have installed it.

Note: Check the power supply requirements in Chapter 25 on page 215, and make sure you are using an appropriate power source.

Keep the power supply switch and the MES-2110's power switch in the OFF position until you come to the procedure for turning on the power.

Use only power wires of the required diameter for connecting the MES-2110 to a power supply.

3.2.1 AC Power Connection

Note: This is only for the AC model of the MES-2110.

Connect the female end of the power cord to the power socket of your MES-2110. Connect the other end of the cord to a power outlet. Make sure that no objects obstruct the airflow of the fans.

3.2.2 DC Power Connection

Note: This is only for the DC model of the MES-2110.

The MES-2110 uses a single ETB series terminal block plug with four pins which allows you to connect up to two separate power supplies. If one power supply fails the system can operate on the remaining power supply. Use two wires to connect to a single terminal pair, one wire for the positive terminal and one wire for the negative terminal.

Note: The current rating of the power wires must be greater than 20 Amps. The power supply to which the MES-2110 connects must have a built-in circuit breaker or switch to toggle the power.

Note: When installing the power wire, push it wire firmly into the terminal as deep as possible and make sure that no exposed (bare) wire can be seen or touched.

An exposed wire from a DC power source can be dangerous. Use extreme care when connecting a DC power source to the device.

To connect a power supply:

1. Use a screwdriver to loosen the terminal block captive screws.
2. Connect one end of a power wire to the MES-2110's **RTN** (return) pin and tighten the captive screw.
3. Connect the other end of the power wire to the positive terminal on the power supply.
4. Connect one end of a power wire to the MES-2110's **-48V** (input) pin and tighten the captive screw.
5. Connect the other end of the power wire to the negative terminal on the power supply.
6. Insert the terminal block plug in the MES-2110's terminal block header.

3.2.3 Powering on the MES-2110

1. Turn on the power supply first.
2. Turn on the MES-2110's power second.

3.3 LEDs

After you connect the power to the MES-2110, view the LEDs to ensure proper functioning of the MES-2110 and as an aid in troubleshooting.

Table 2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	On	The system is on and functioning properly.
		Blinking	The system is rebooting and performing self-diagnostic tests.
		Off	The power is off or the system is not ready/malfunctioning.
Ethernet Ports			
LINK/ ACT	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		On	The link to a 10 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
Mini-GBIC Slots			
LNK	Green	On	The link to this port is up.
		Off	The link to this port is not connected.
ACT	Green	On	The link to an Ethernet network is on.
		Blinking	This port is receiving or transmitting data.
		Off	The port is not receiving or transmitting data.
1000Base-T Ethernet Ports (in Dual Personality Interface)			

Table 2 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
ACT	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps or a 1000 Mbps Ethernet network.
		On	The link to a 10 Mbps or a 1000 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.

4

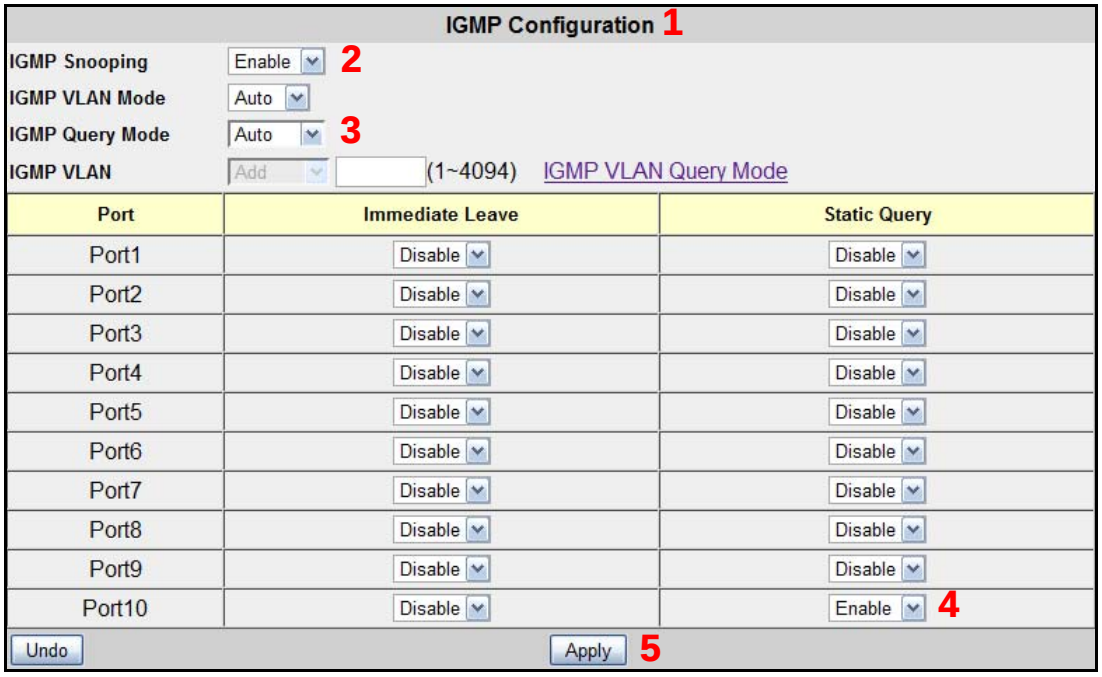
Tutorials

4.1 IGMP Snooping

IGMP snooping allows a layer-2 device such as the MES-2110 to eavesdrop on IGMP-based data packets traversing the communications channel on layer-3. This allows it to determine which ports should specifically receive multicast traffic in order to prevent multicasting flooding across all of its ports.

This tutorial shows you how to enable IGMP snooping, set IGMP to automatic query mode, and then set port 10 to static.

To configure IGMP snooping:



1 In the Web Configurator, open the **Configuration > IGMP Menu > IGMP Configuration** screen.

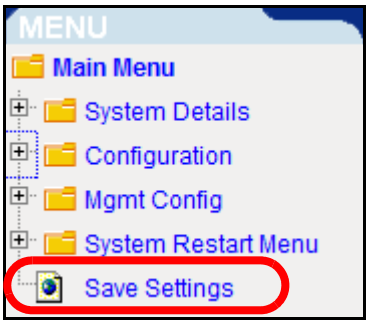
2 Set **IGMP Snooping** to **Enable**.

3 Set **IGMP Query Mode** to **Auto**.

4 Set the **Static Query** field for port 10 to **Enable**.

5 Click **Apply**. The new settings appear in the **IGMP Status** table.

6 Click **Save Settings** in the navigation panel to store the changes permanently.



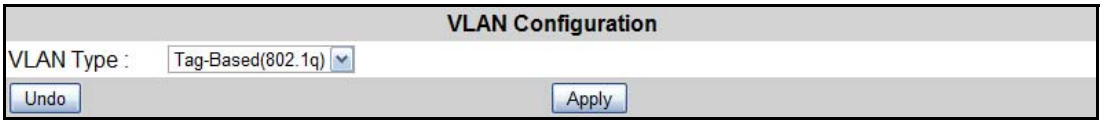
4.2 RADIUS Configuration

RADIUS is a protocol explicitly designed to manage single location authentication and authorization for an entire network. It also provides accounting services for client usage of network resources.

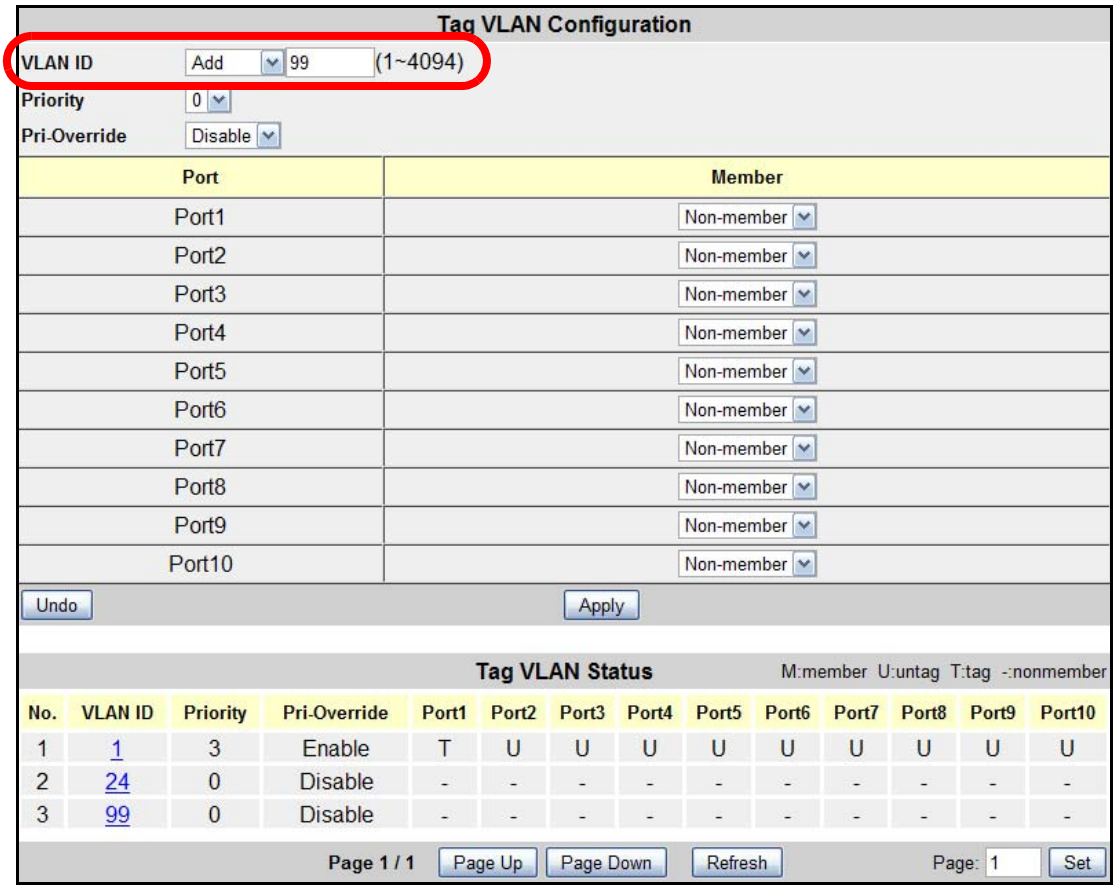
This tutorial shows you how to set up one RADIUS server (172.16.10.10) and a shared secret key (“hello”) for authentication.

To assign a RADIUS server to the MES-2110:

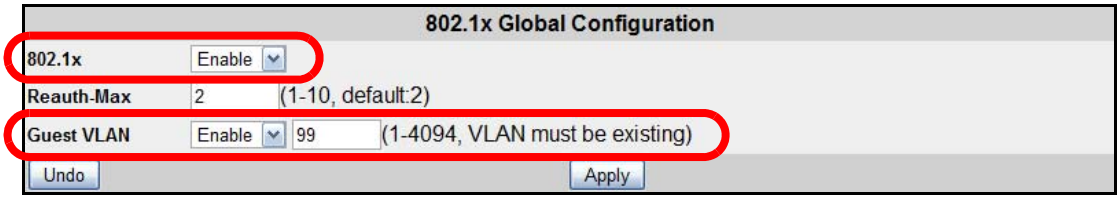
1 Open the **Configuration > VLAN Menu > VLAN Type** menu, set **VLAN Type** to **Tag-Based(802.1q)**, then click **Apply**.



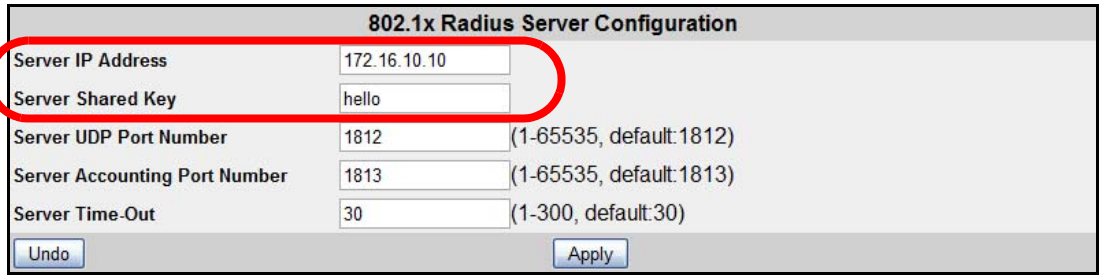
2 On the **Configuration > VLAN Menu > Tag-Based(802.1q) > Tag-Based info.** screen, add VLAN ID 99 and click **Apply**. The new VLAN ID appears in the **Tag VLAN Status** table.



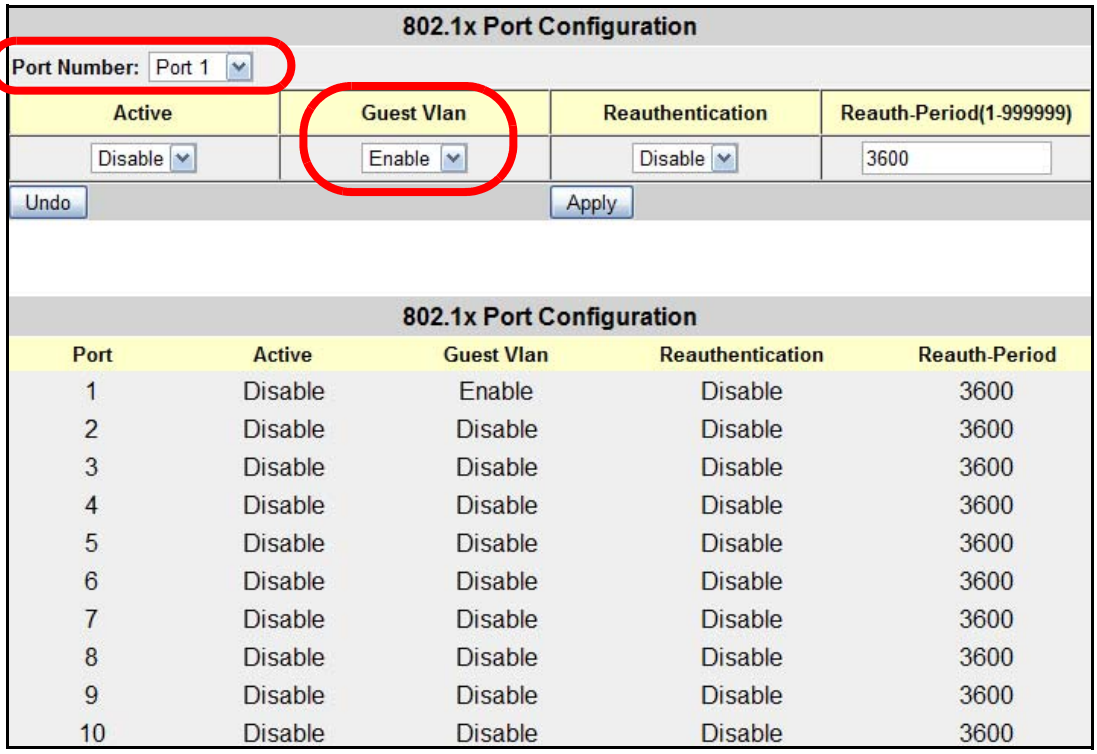
3 Open the **Configuration > 802.1x > Global Configuration** screen. For the **802.1x** option, select **Enable**. For the Guest VLAN option, select **Enable** and enter *99* in the associated field. Click **Apply** to save these changes.



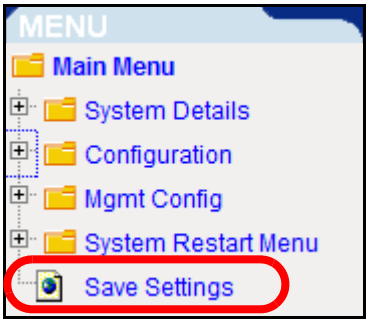
4 Next go to the **Configuration > 802.1x > RADIUS Server Configuration** screen. For **Server IP Address**, enter *172.16.10.10* and for **Shared Server Key** enter *hello*, then click **Apply**.



5 Finally, open the **Configuration > 802.1x > Port Configuration** screen. From the **Port Number** menu select **Port 1** if not already selected, set the **Guest VLAN** option to **Enable**, and click **Apply**.



6 Click **Save Settings** in the navigation panel to store the changes permanently.



4.3 MVR Configuration

MVR manages multicast traffic from an upstream VLAN on a multicast server to downstream subscribers in the same VLAN group. This allows you to regulate bandwidth by not streaming multicast traffic to every device on your network but rather just to the intended computers.

This tutorial shows you set up a Multicast VLAN Registration (MVR) group and then direct all multicast traffic with matching VLAN IDs to it.

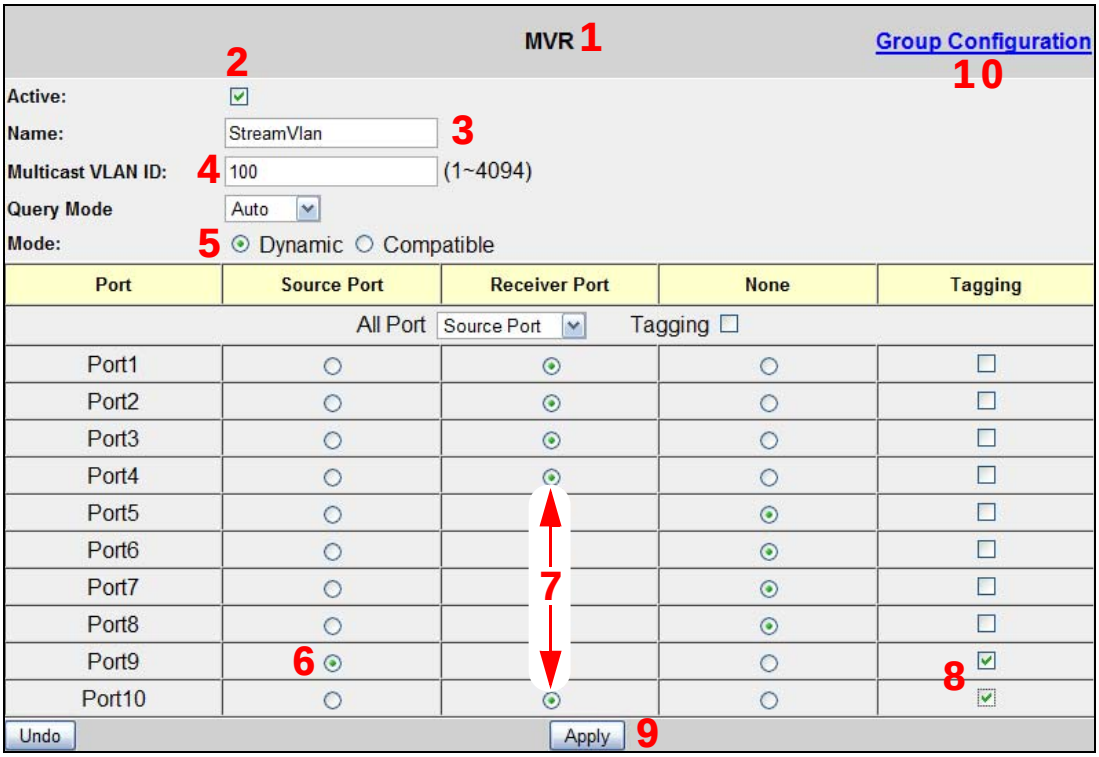
For the purposes of this tutorial, use the following settings:

Table 3 MVR Tutorial Values

SETTING	VALUE
VLAN Name	StreamVlan
VLAN ID	100
Source Port	9
Receiver Ports	1-4, 10
Multicast Group Mode	Dynamic
Tagging Ports	9, 10
Multicast Group IP Addresses	223.3.3.1 ~ 223.3.3.10
Multicast Group ID	1

Note: Make sure your **Configuration > VLAN Menu > VLAN Type** is set to **Tag-Based(802.1q)** before proceeding.

To configure MVR:



1 Open the **Configuration > IGMP Menu > MVR** screen.

2 Select **Active** to enable the MVR feature.

3 Enter StreamVlan as the MVR **Name**.

4 Enter 100 as the **Multicast VLAN ID**.

5 Set the MVR **Mode** to **Dynamic**.

6 In the **Source Port** column, deselect all ports except **Port 9**. This will be the source port which receives all incoming multicasts from upstream.

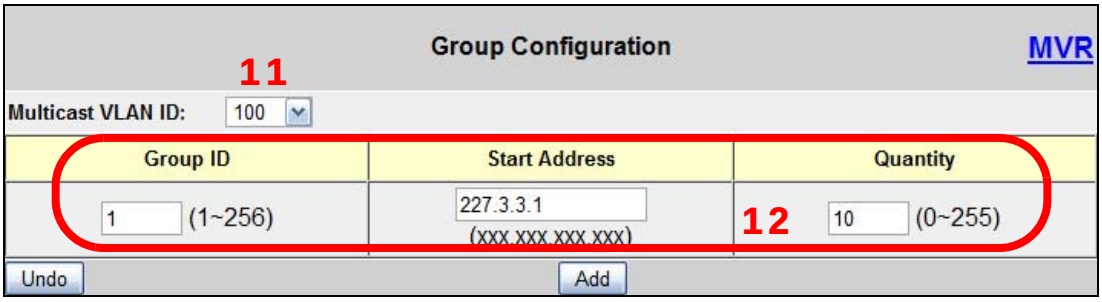
7 In the **Receiver Port** column, select **Ports 1-4** and **Port 10**. These ports are now the designated downstream recipients for all incoming multicasts.

8 In the **Tagging** column, enable tagging for **Port 9** and **10**.

9 Click **Apply** to store these changes.

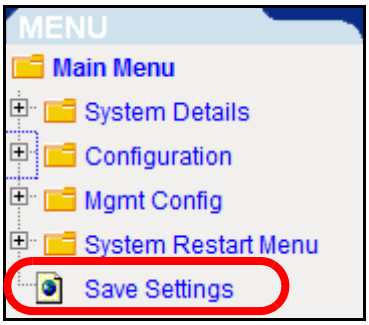
10 Click the **Group Configuration** link.

11 In the **Group Configuration** screen, select the **Multicast VLAN ID** you created in step 4 from the list. In this example, it is VLAN ID 100.



12 Enter a **Group ID** of 1, a **Start Address** of 227.3.3.1, and a **Quantity** of 10.

13 Click **Add**, then click **Save Settings** in the navigation panel to store the changes permanently.

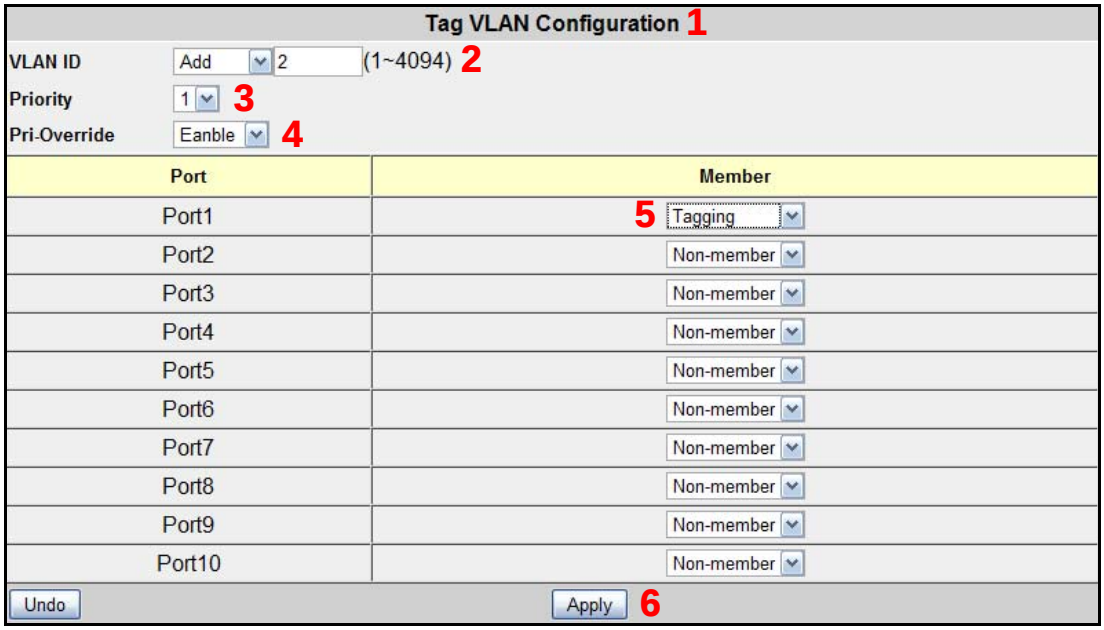


4.4 VLAN ID Priority

This tutorial assigns port 1 as a tagged port for VLAN 1 and sets the priority of all incoming packets from VLAN 1 to priority 3.

Note: Make sure your **Configuration > VLAN Menu > VLAN Type** is set to **Tag-Based(802.1q)** before proceeding.

To configure VLAN ID priority:



1 Open the **Configuration > VLAN Menu > Tag-Based(802.1q) > Tag-Based info.** screen.

2 For **VLAN ID**, select **Add** from the menu and enter 2 in the associated field.

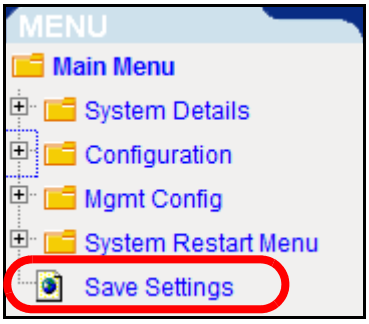
3 Set the **Priority** to 1.

4 For **Pri-Overide**, select **Enable**.

5 In the **Member** column for **Port 1**, select **Tagging**.

6 Click **Apply**.

7 Click **Save Settings** in the navigation panel to store the changes permanently.

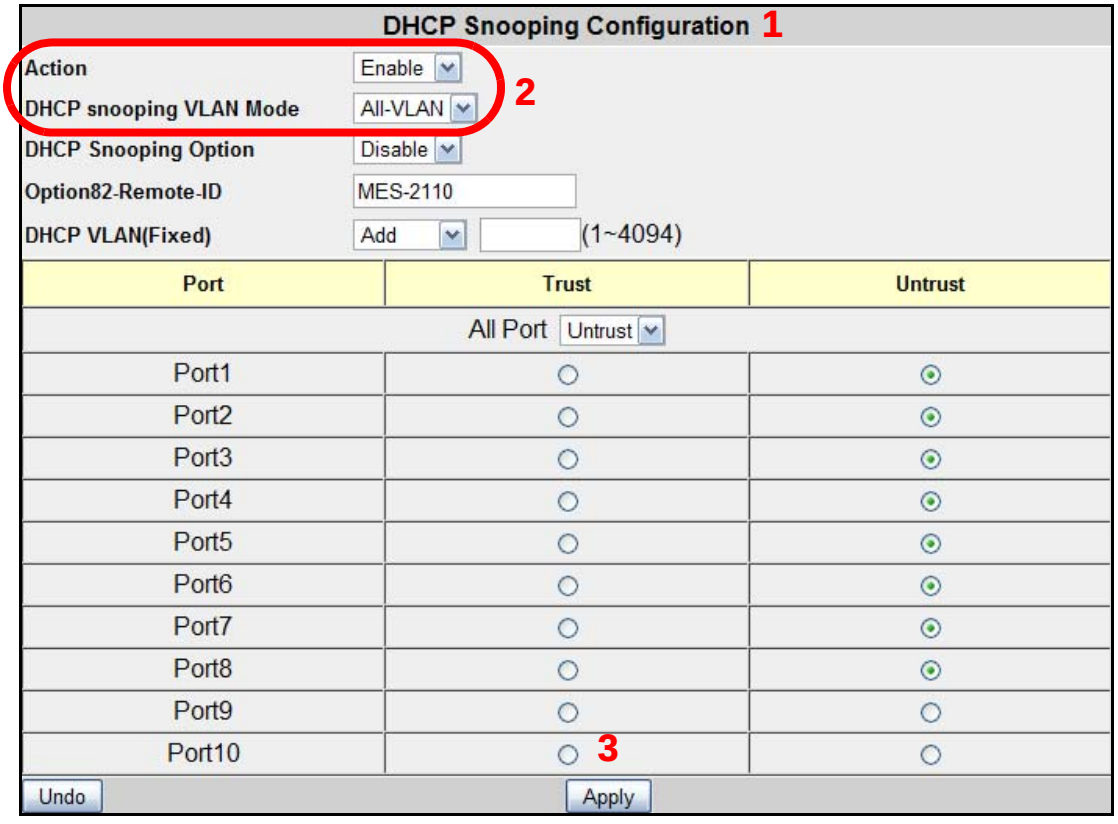


4.5 Untrusted ARP Inspection

This tutorial shows you how to assign port 1 to 8 as untrusted for ARP inspection. Generally if you want to enable ARP inspection on the device you also have to enable DHCP snooping first to build a binding table.

To set up ARP inspection:

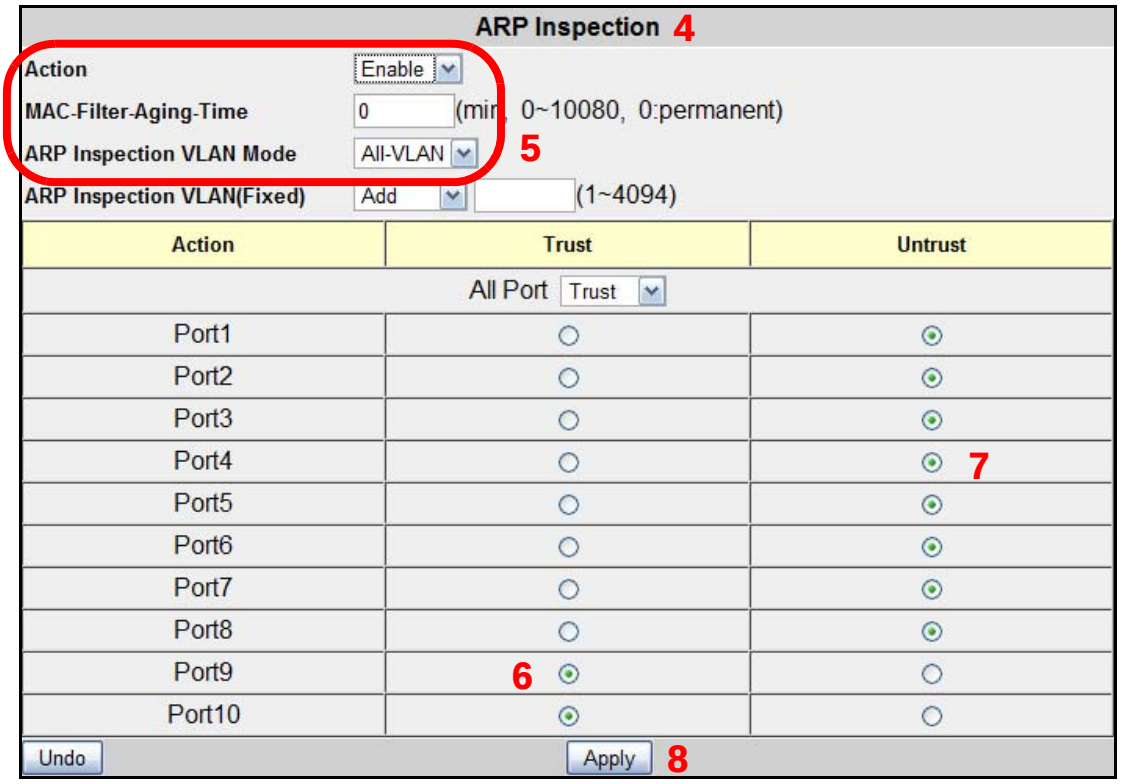
1 Open the **Configuration > IP Source Guard > DHCP > DHCP Snooping Configuration** screen.



2 Set **Action** to **Enable** and **DHCP Snooping VLAN Mode** to **All-VLAN**.

3 Click **Apply**.

4 Open the **Configuration > IP Source Guard > ARP Inspection > ARP Inspection Configuration** screen.



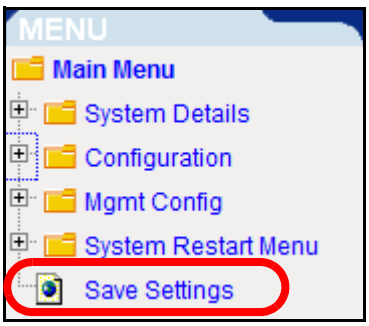
5 Set **Action** to **Enable** and **ARP Inspection VLAN Mode** to **All-VLAN**.

6 In the **Trust** column, select **Port 9** and **Port 10**.

7 In the **Untrust** column, select **Ports 1-8**.

8 Click **Apply**.

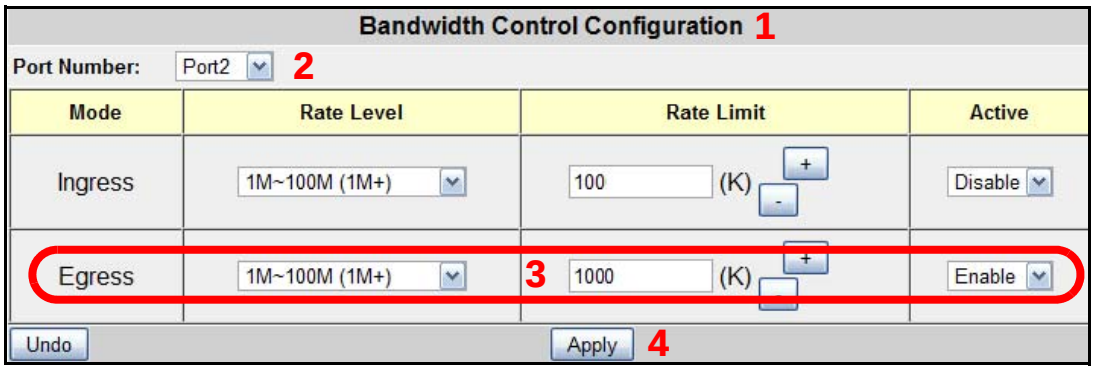
9 Click **Save Settings** in the navigation panel to store the changes permanently.



4.6 Outgoing Traffic Bandwidth

This tutorial shows you how to set the outgoing traffic bandwidth limit to 1 Mbps for Port 2.

To configure outgoing traffic bandwidth:



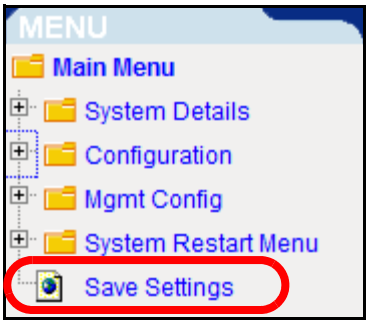
1 Open the **Configuration > Bandwidth Control** screen.

2 Set the **Port Number** to **Port 2**.

3 In the **Egress** row, set the **Rate Level** to **1M~100M (1M+)**, the **Rate Limit** to 1000 k, and the **Active** option to **Enable**.

4 Click **Apply**.

5 Click **Save Settings** in the navigation panel to store the changes permanently.

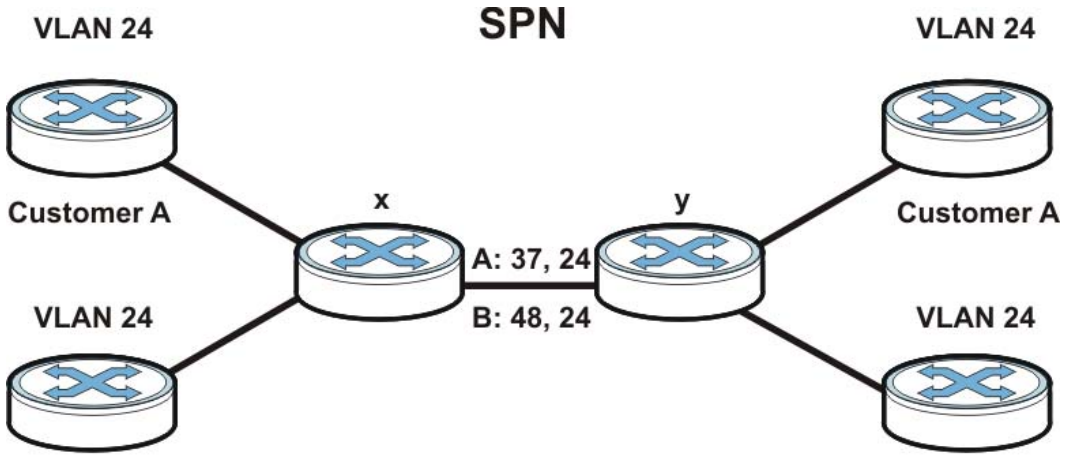


4.7 Frame Tagging

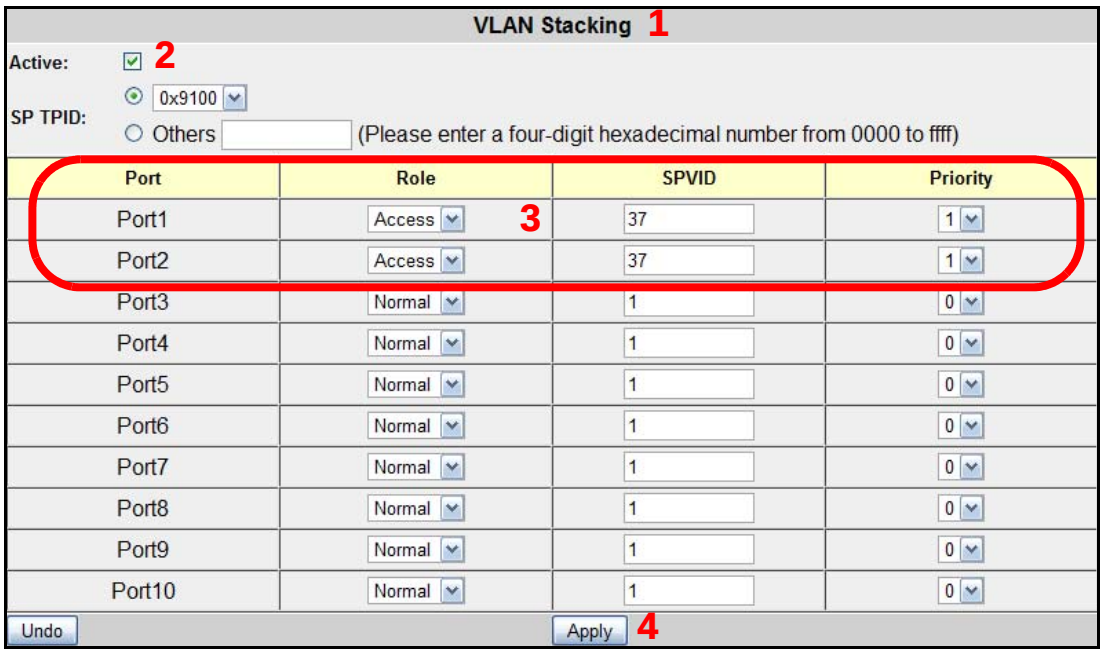
In this tutorial, shows you how to configure ports 1 and 2 on the switch to tag incoming frames with the service provider's VID of 37 (ports are connected to customer A network) and how to set the priority for ports 1 and 2 to 3.

The scenario is that both A and B are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer A and tag 48 to distinguish customer B at edge device x and then stripping those tags at edge device y as the data frames leave the network.

Figure 15 Frame Tagging Example



To configure frame tagging:



1 Open the **Configuration > VLAN Menu > Tag-Based(802.1q) > VLAN Stacking** screen.

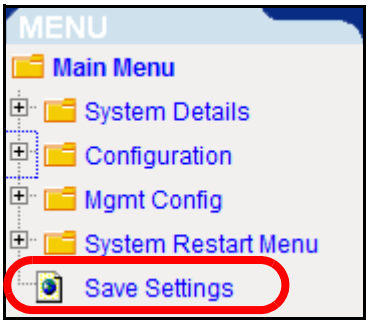
2 Select **Active** and click **Apply**.

3 For **Port 1** and **Port 2**, use the following settings: for **Role** select **Access**, for **PVID** use 37 and for **Priority** choose 1.

Note: If the port for which you are configuring frame tagging is the same port by which you connect to the MES-2110 then your computer should use the same PVID or you should switch a non-tagged port.

4 Click **Apply**.

5 Click **Save Settings** in the navigation panel to store the changes permanently.



5

The Web Configurator

5.1 Introduction

This section introduces the configuration and functions of the web configurator.

The web configurator is an HTML-based management interface that allows easy MES-2110 setup and management via Internet browser. Use Internet Explorer 6.0 and later or Firefox 1.5 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

5.2 System Login

1. Start your web browser.
2. Type “http://” and the IP address of the MES-2110 (for example, the default is 192.168.1.1) in the Location or Address field. Press [ENTER].

3 The login screen appears. Enter the user name (**admin** by default) and password (**1234** by default).

Figure 16 Web Configurator: Login

Connect to 192.168.1.1
The server 192.168.1.1 at Web Manager requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

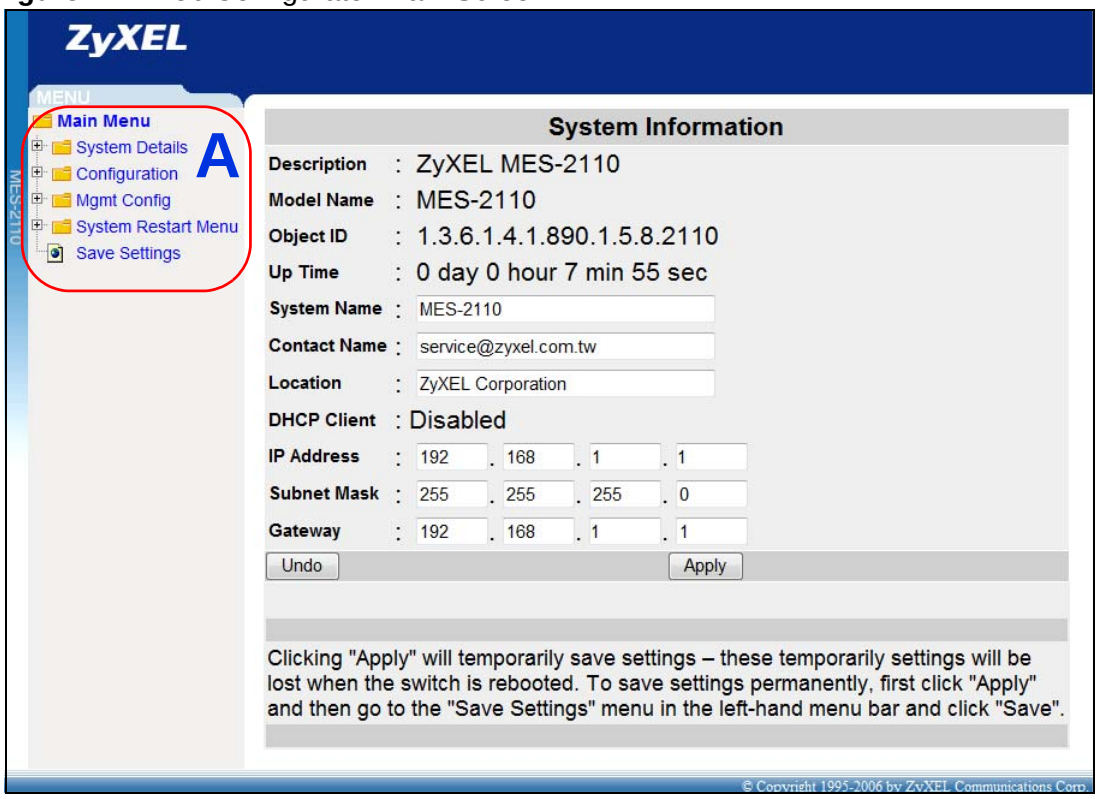
4 Click **OK** to view the first web configurator screen.

5.3 The Main Screen

The **Main** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

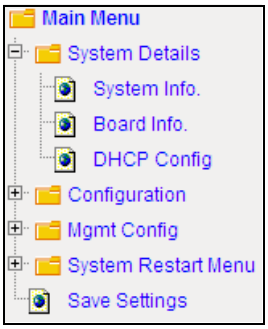
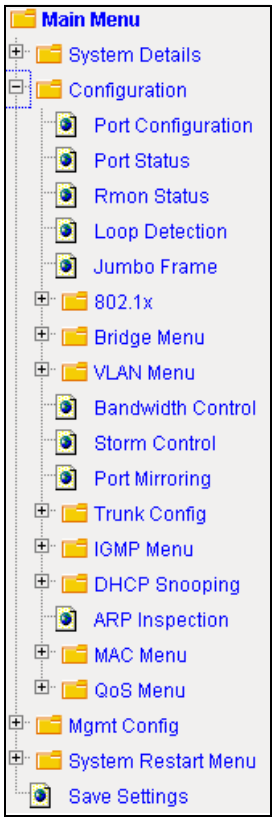
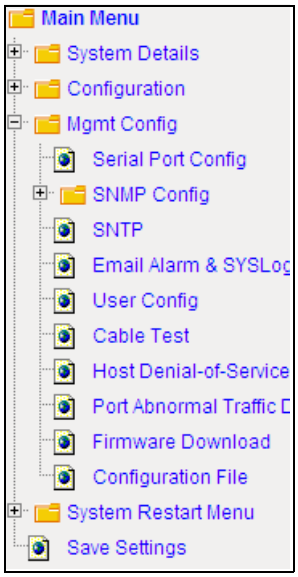
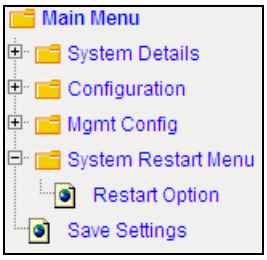
Figure 17 Web Configurator Main Screen


ZyXEL
MENU
Main Menu
System Details
Configuration
Mgmt Config
System Restart Menu
Save Settings
A
MES-2110
System Information
Description : ZyXEL MES-2110
Model Name : MES-2110
Object ID : 1.3.6.1.4.1.890.1.5.8.2110
Up Time : 0 day 0 hour 7 min 55 sec
System Name : MES-2110
Contact Name : service@zyxel.com.tw
Location : ZyXEL Corporation
DHCP Client : Disabled
IP Address : 192 . 168 . 1 . 1
Subnet Mask : 255 . 255 . 255 . 0
Gateway : 192 . 168 . 1 . 1
Undo
Apply
Clicking "Apply" will temporarily save settings – these temporarily settings will be lost when the switch is rebooted. To save settings permanently, first click "Apply" and then go to the "Save Settings" menu in the left-hand menu bar and click "Save".
© Copyright 1995-2006 by ZyXEL Communications Corp.

A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 4 Navigation Panel Sub-links Overview

SYSTEM DETAILS	CONFIGURATION	MGMT CONFIG	SYSTEM RESTART MENU
			

The following table lists the various web configurator screens within the sub-links.

Table 5 Web Configurator Screen Sub-links Details

SYSTEM DETAILS	CONFIGURATION	MGMT CONFIG	SYSTEM RESTART MENU
System Info. Board Info. DHCP Config	Port Configuration Port Status Rmon Status Loop Detection Jumbo Frame 802.1 Global Configuration RADIUS Server Configuration Port Configuration 802.1x Status Bridge Menu Bridge Config RSTP System Config RSTP Per Port Config VLAN Menu VLAN Type Port-Based Tag-Based (802.1q) VLAN Stacking Port Info. Tag-Based Info. Management VLAN Bandwidth Control Storm Control Port Mirroring Trunk Config Aggregator Setting LACP Configuration LACP Link Status IGMP Menu IGMP Config IGMP Groups Status MVR	Serial Port Config SNMP Config SNMP Communities IP Trap Manager SNTP Email Alarm & SYSLog User Config Cable Test Host Denial-of-Service Protection Port Abnormal Traffic Detection Firmware Download Configuration File	Restart Option

	DHCP Snooping DHCP Snooping Config DHCP Binding Table ARP Inspection MAC Menu MAC Table Status Lock Learning MAC MAC Filter Config MAC Limit Config QoS Menu Base Configuration 802.1p Priority Tag Priority IP DSCP Priority Priority Override Configuration		

The following table describes the links in the navigation panel.

Table 6 Navigation Panel Links

LINK	DESCRIPTION
System Details	
System Info.	This link takes you to a screen that displays general system information. You can also configure general system information about the MES-2110.
Board Info.	This link takes you to a screen that shows hardware and firmware information.
DHCP Config	This link takes you to a screen where you can configure the DHCP settings.
Configuration	
Port Configuration	This link takes you to a screen where you can configure settings for individual MES-2110 ports.
Port Status	This link takes you to a screen that shows port settings for individual MES-2110 ports.
Rmon Status	This link takes you to a screen where you can view statistics on the traffic going through each port.
Loop Detection	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
Jumbo Frame	This link takes you to a screen where you can configure Jumbo frames or Ethernet frames with a payload greater than 1500 bytes.Use this screen to configure the jumbo frame size.
802.1x	This link takes you to a screen where you can configure IEEE 802.1x authentication.
Bridge Menu	This link takes you to screens where you can configure the RSTP to prevent network loops.
VLAN Menu	This link takes you to screens where you can configure port-based or tag-based (802.1Q) VLAN (depending on what you configured in the Switch Setup menu).

Table 6 Navigation Panel Links (continued)

LINK	DESCRIPTION
Bandwidth Control	This link takes you to a screen where you can configure bandwidth limits on the MES-2110.
Storm Control	This link takes you to a screen to set up broadcast filters.
Port Mirroring	This link takes you to a screen where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Trunk Config	This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link.
IGMP Menu	This link takes you to screens where you can configure various multicast features, IGMP snooping and create multicast VLANs.
DHCP Snooping	This link takes you to screens where you can configure filtering of unauthorized DHCP frames in your network.
ARP Inspection	This link takes you to a screen where you can configure filtering of unauthorized Address Resolution Protocol (ARP) frames in your network.
MAC Menu	This link takes you to screens where you can configure the following settings: • configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating via the MES-2110, • activate MAC address learning and set the maximum number of MAC addresses to learn on a port, • view the MAC addresses (and types) of devices attached to what ports.
QoS Menu	This link takes you to screens where you can configure priority levels for traffic transmitted through each port.
Mgmt Config	
Serial Port Config	This link takes you to a screen where you can configure the parameters for connections via the console port.
SNMP Config	This link takes you to screens where you can configure settings for date and time.
SNTP	This link takes you to a screen where you can configure SNTP and date/time settings.
Email Alarm & SYSLog	This link takes you to screens where you can set up system logs and e-mail the logs to you.
User Config	This link takes you to a screen where you can set up administrative and user accounts for people to use the MES-2110.
Cable Test	This link takes you to a screen where you can test the cable connection on each port.
Host Denial-of-Service Protection	This link takes you to a screen where you can allow trusted computers to access the MES-2110 via remote management.
Port Abnormal Traffic Detection	This link takes you to a screen where you can configure the MES-2110 to detect abnormal traffic transmission and temporarily or permanently block traffic transmission through a port.

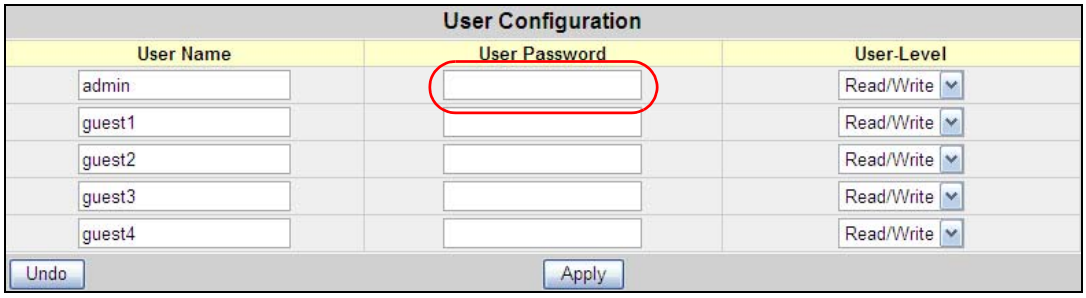
Table 6 Navigation Panel Links (continued)

LINK	DESCRIPTION
Firmware Download	This link takes you to a screen where you can perform firmware maintenance.
Configuration File	This link takes you to a screen where you can perform configuration file maintenance.
System Restart Menu	
Restart Option	This link takes you to a screen where you can reboot the system.
Save Settings	This link takes you to a screen where you can save the changes you have made on the MES-2110 and restart the MES-2110.

5.3.1 Set Up the Administrative Password

After you log in for the first time, it is recommended you set up an administrator password. Click **Mgmt Config** > **User Config** to display the next screen. Enter a password for the **admin** account and click **Apply**.

Figure 18 Configure Administrator Login Password



5.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the MES-2110's power is turned off.

Click the **Save Settings** link in the navigation panel to save your configuration to nonvolatile memory. Nonvolatile memory refers to the MES-2110's storage that remains even if the MES-2110's power is turned off. If you don't use **Save Settings** all configuration changes will only apply until you restart the MES-2110.

Note: Use the **Save Settings** link when you are done with a configuration session.

Note: After saving changes to the IP Address, Subnet Mask or Gateway settings, the MES-2110 will need to reboot to put them into effect (after prompting you for confirmation.)

5.5 Switch Lockout

You could block yourself (and all others) from using in-band-management (managing through the data ports) if you do one of the following:

1. Delete the management VLAN (default is VLAN 1).
2. Delete all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the MES-2110.
3. Filter all traffic to the CPU port.
4. Disable all ports.
5. Misconfigure the text configuration file.
6. Forget the password and/or IP address.
7. Prevent all services from accessing the MES-2110.
8. Change a service port number but forget it.

Note: Be careful not to lock yourself and others out of the MES-2110. If you do lock yourself out, try using out-of-band management (via the console port) to configure the MES-2110.

5.6 Resetting the MES-2110

If you lock yourself (and others) from the MES-2110 or forget the administrator password, you will need to reload the factory-default configuration file or reset the MES-2110 back to the factory defaults.

5.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600 bps with 8 data bits, no parity, one stop bit and flow control set to none. The password will also be cleared and the IP address be set to 192.168.0.254.

To upload the configuration file, do the following:

1. Connect to the console port using a computer with terminal emulation software.

2 Disconnect and reconnect the MES-2110's power to begin a session. When you reconnect the MES-2110's power, you will see the initial screen.

3 When you see "Username:", type admin and press [Enter].

4 Type the administrative password and press [Enter]. Simply press [Enter] if you did not set up a password.

5 Type enable and press [Enter] to turn on administrative commands.

6 Type reset default and press [Enter] to restore the system to the factory defaults. The MES-2110 will restart.

Figure 19 Resetting the MES-2110: Via the Console Port

```
Username: admin
Password:
MES-2110> enable

MES-2110# reset default
```

The MES-2110 is now reinitialized with a default configuration file.

6

System Details

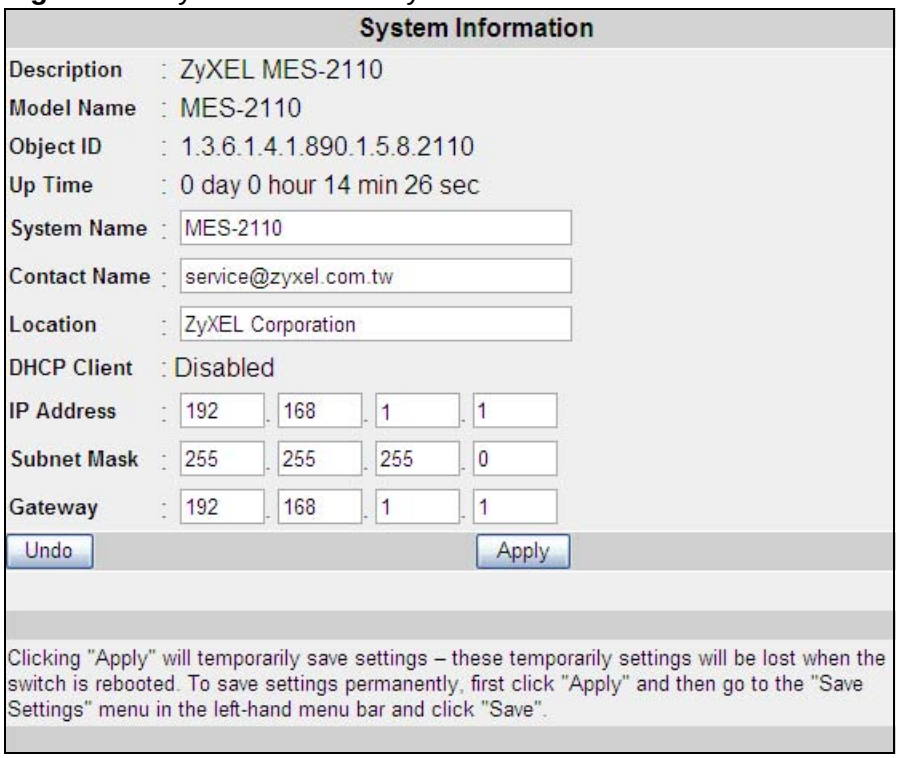
6.1 Overview

The **System Details** screens show general system information about the MES-2110. You can also use the screens to configure system and DHCP client settings.

6.2 The System Information Screen

Click **System Details** > **System Info.** to open the following screen.

Figure 20 System Details > System Info.


System Information
Description : ZyXEL MES-2110
Model Name : MES-2110
Object ID : 1.3.6.1.4.1.890.1.5.8.2110
Up Time : 0 day 0 hour 14 min 26 sec
System Name : MES-2110
Contact Name : service@zyxel.com.tw
Location : ZyXEL Corporation
DHCP Client : Disabled
IP Address : 192 . 168 . 1 . 1
Subnet Mask : 255 . 255 . 255 . 0
Gateway : 192 . 168 . 1 . 1
Undo
Apply
Clicking "Apply" will temporarily save settings – these temporarily settings will be lost when the switch is rebooted. To save settings permanently, first click "Apply" and then go to the "Save Settings" menu in the left-hand menu bar and click "Save".

The following table describes the labels in this screen.

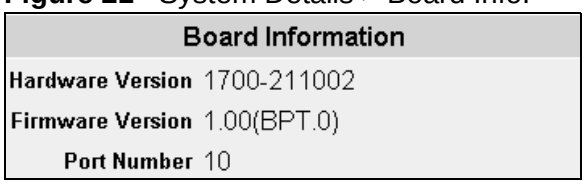
Table 7 System Details > System Info.

LABEL	DESCRIPTION
Description	This is the descriptive name of the MES-2110 for identification purposes.
Model Name	This is the model name of the MES-2110.
Object ID	An Object ID defines what trap the MES-2110 should send an SNMP Manager.
Up Time	This shows how long the MES-2110 has been turned on.
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Contact Name	Enter the name of the person in charge of this MES-2110. You can use up to 32 printable ASCII characters; spaces are allowed.
Location	Enter the geographic location of your MES-2110. You can use up to 32 printable ASCII characters; spaces are allowed.
DHCP Client	This shows whether the DHCP client is **Enabled** or **Disabled**. If DHCP is disabled, you must enter an IP address, subnet mask and gateway in the following fields. Otherwise, a DHCP server will assign this information to the MES-2110. See Section 6.4 on page 63 for details about configuring the DHCP client.
IP Address	Enter the IP address of your MES-2110 in dotted decimal notation for example 192.168.1.1.
Subnet Mask	Enter the IP subnet mask of your MES-2110 in dotted decimal notation for example 255.255.255.0.
Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

6.3 The Board Information Screen

Use this screen to view the hardware and firmware information. Click **System Details** > **Board Info.** to open the following screen.

Figure 21 System Details > Board Info.



The following table describes the labels in this screen.

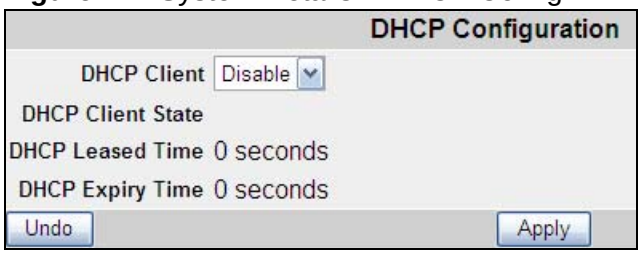
Table 8 System Details > Board Info.

LABEL	DESCRIPTION
Hardware Version	This is the version number of the MES-2110's hardware.
Firmware Version	This is the version number of the MES-2110's current firmware including the date and time that the firmware is created.
Port Number	This shows the number of available ports on the MES-2110.

6.4 The DHCP Configuration Screen

Use this screen to turn on or off the DHCP client. Click **System Details** > **DHCP Config** to open the following screen.

Figure 22 System Details > DHCP Config



The following table describes the labels in this screen.

Table 9 System Details > DHCP Config

LABEL	DESCRIPTION
DHCP Client	Use this to turn the DHCP client on or off. Turn on the DHCP client if you have a DHCP server that can assign the MES-2110 an IP address, subnet mask and a default gateway IP address automatically.
DHCP Client State	This shows whether the DHCP client is **Enabled** or **Disabled**.
DHCP Leased Time	This is how long ago the MES-2110 got an IP address from a DHCP server (if DHCP client is enabled).
DHCP Expiry Time	This is how long there is to go before the MES-2110 will get a new IP address from a DHCP server (if DHCP client is enabled).
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

Once you click the **Apply** button, the following message displays, reminding you to save your settings in the **Save Settings** screen and reboot the MES-2110.

Figure 23 System Details > DHCP Config > Apply

Windows Internet Explorer
For the DHCP Client changes take effect,
go to the "Save Settings" menu and click "Save".
The switch will immediately reboot.
OK

7

Configuration

7.1 Overview

The **Configuration** screens let you configure the MES-2110 settings.

7.2 The Port Configuration Screen

Use this screen to configure MES-2110 port settings. You can assign a unique name to the ports, select its speed setting and enable or disable auto-negotiation. Click **Configuration** > **Port Configuration** to open the following screen.

Figure 24 Configuration > Port Configuration

Port Configuration

Port Number: Port1

Name	Admin	Speed	Duplex	AUTO	Flow-Control
	Enabled	100M	Full	Enabled	Enabled

Undo Apply

Port Configuration

Port	Name	Admin	Speed	Duplex	AUTO	Flow-Control
Port1		Enable	100M	Full	On	Enable
Port2		Enable	100M	Full	On	Enable
Port3		Enable	100M	Full	On	Enable
Port4		Enable	100M	Full	On	Enable
Port5		Enable	100M	Full	On	Enable
Port6		Enable	100M	Full	On	Enable
Port7		Enable	100M	Full	On	Enable
Port8		Enable	100M	Full	On	Enable
Port9		Enable	1000M	Full	Off	Enable
Port10		Enable	1000M	Full	Off	Enable

The following table describes the labels in this screen.

Table 10 Configuration > Port Configuration

LABEL	DESCRIPTION
Port	This is the port number.
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some Web Configurator screens.
Admin	Use this to enable or disable administrative access through this port.
Speed	Select the port's current speed (**10M** for 10 Mbps and **100M** for 100 Mbps). The speed for the fiber ports is fixed.
Duplex	Use this field to change the status to **Half** or **Full** duplex mode. The duplex status for the fiber ports is fixed.
AUTO	Use this to enable or disable auto-negotiation. **AUTO** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the MES-2110 negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the MES-2110 determines the connection speed by detecting the signal on the cable and using half duplex mode. When the MES-2110's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow-Control	Use this to enable or disable flow control. A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing frame discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The MES-2110 uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of frame collision) causing the sending port to temporarily stop sending signals and resend later.
Port	This indicates the port number
Name	This indicates the descriptive named assigned to the port.
Admin	This indicates whether administrative access is enabled or disabled for this port.
Speed	This indicates the speed assigned to the port (**10M** for 10 Mbps and **100M** for 100 Mbps).

Table 10 Configuration > Port Configuration

LABEL	DESCRIPTION
Duplex	This indicates the port's duplex mode (**Half** or **Full**).
AUTO	This indicates whether auto-negotiation for this port is enabled or disabled.
Flow-Control	This indicates whether flow control for this port is enabled or disabled.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

7.3 The Port Status Screen

To view the port statistics, click **Configuration** > **Port Status** to display the **Status** screen as shown next.

Figure 25 Configuration > Port Status

Ports Status

Port	Name	Type	Admin	Speed	Duplex	Link	AUTO	Flow-Control
Port1		RJ45	Enabled	100M	Full	Up	On	Enabled
Port2		RJ45	Enabled	100M	Full	Down	On	Enabled
Port3		RJ45	Enabled	100M	Full	Down	On	Enabled
Port4		RJ45	Enabled	100M	Full	Down	On	Enabled
Port5		RJ45	Enabled	100M	Full	Down	On	Enabled
Port6		RJ45	Enabled	100M	Full	Down	On	Enabled
Port7		RJ45	Enabled	100M	Full	Down	On	Enabled
Port8		RJ45	Enabled	100M	Full	Down	On	Enabled
Port9		Fiber	Enabled	1000M	Full	Down	On	Enabled
Port10		Fiber	Enabled	1000M	Full	Down	On	Enabled

Port Configuration

The following table describes the labels in this screen.

Table 11 Configuration > Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Name	This is the name you assigned to this port in the **Configuration** > **Port Configuration** screen.
Type	This is the type of connector for each port. Port 1-8 are RJ-45 ports for Ethernet connections. Port 9-10 are Gigabit SFP ports for fiber connections.
Admin	This shows whether administrative access is **Enabled** or **Disabled** on the port. When administrative access is disabled on the port, users cannot manage the MES-2110 via that port.

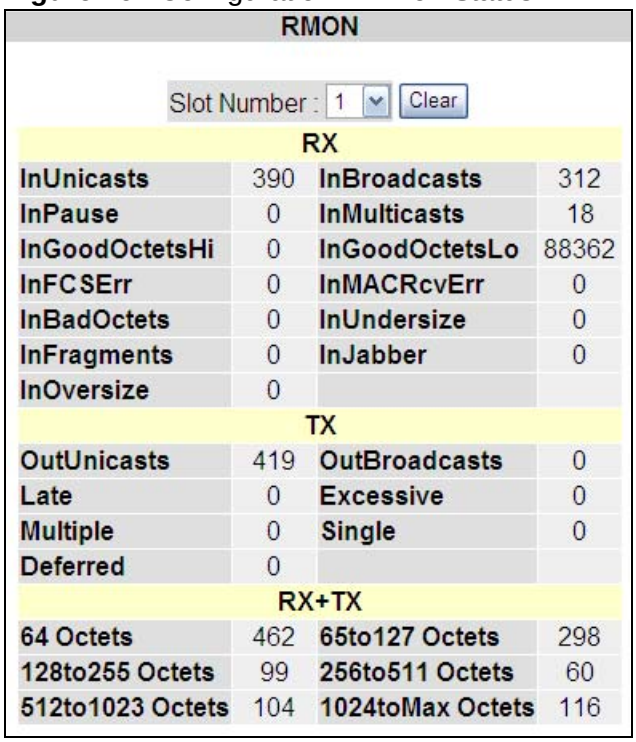
Table 11 Configuration > Port Status (continued)

LABEL	DESCRIPTION
Speed	This is the port's current speed (**10M** for 10 Mbps and **100M** for 100 Mbps).
Duplex	This is the the port's duplex status (**Half** or **Full**).
Link	This shows the port's connection status.
AUTO	This shows whether auto-negotiation is **On** or **Off**.
Flow-Control	This shows whether flow control is **Enabled** or **Disabled**.
Port Configuration	Click this to configure port settings in the **Port Configuration** screen.

7.4 The RMON Status Screen

Use this screen to view individual port statistics. Click **Configuration** > **Rmon Status** to open the following screen.

Figure 26 Configuration > Rmon Status



The following table describes the labels in this screen.

Table 12 Configuration > Rmon Status

LABEL	DESCRIPTION
Slot Number	Use this to select the port number you are viewing.
Clear	Click this to reset the statistics on this port to zero.

Table 12 Configuration > Rmon Status (continued)

LABEL	DESCRIPTION
RX The following fields show detailed information about frames received.	
InUnicasts	This field shows the number of good unicast frames received.
InBroadcasts	This field shows the number of good broadcast frames received.
InPause	This field shows the number of 802.3x Pause frames received.
InMulticasts	This field shows the number of good multicast frames received.
InGoodOctetsHi	This field shows the number of good upper octet frames received.
InGoodOctetsLo	This field shows the number of good lower octet frames received.
InFCSErr	This field shows the number of frames received with Cyclic Redundant Check (CRC) error(s).
InMACRcvErr	This field shows the number of frames received with an RxErr signal from the PHY.
InBadOctets	This field shows the number of bad octet frames received.
InUndersize	This field shows the number of frames received that were too short (shorter than 64 octets).
InFragments	This field shows the number of frames received that were too short (shorter than 64 octets) and were received with with Cyclical Redundancy Check (CRC) errors.
InJabber	This field shows the number of frames received with a length that exceeds the maximum octet size and were received with CRC errors.
InOversize	This field shows the number of frames received with a length that was out of range.
TX The following fields show detailed information about frames transmitted.	
OutUnicasts	This field shows the number of good unicast frames transmitted.
OutBroadcasts	This field shows the number of good broadcast frames transmitted.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the frames have already been transmitted.
Excessive	This is a count of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Multiple	This is a count of successfully transmitted frames for which transmission was inhibited by more than one collision.
Single	This is a count of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Deferred	This is a count of frames for which transmission delayed due to busy traffic. The deferred frames are waiting to be transmitted from the MES-2110 buffer. This counter only works for the half-duplex mode.
RX+TX	
64 Octets	This field shows the number of frames (including bad frames) received that were 64 octets in length.
65to127 Octets	This field shows the number of frames (including bad frames) received that were between 65 and 127 octets in length.

Table 12 Configuration > Rmon Status (continued)

LABEL	DESCRIPTION
128to255 Octets	This field shows the number of frames (including bad frames) received that were between 128 and 255 octets in length.
256to511 Octets	This field shows the number of frames (including bad frames) received that were between 256 and 511 octets in length.
512to1023 Octets	This field shows the number of frames (including bad frames) received that were between 512 and 1023 octets in length.
1024toMax Octets	This field shows the number of frames (including bad frames) received that were between 1024 and the maximum octets in length.

8

Loop Detection

8.1 Overview

Loop detection allows you to configure the MES-2110 to shut down a port if it detects that frames sent out on that port loop back to the MES-2110.

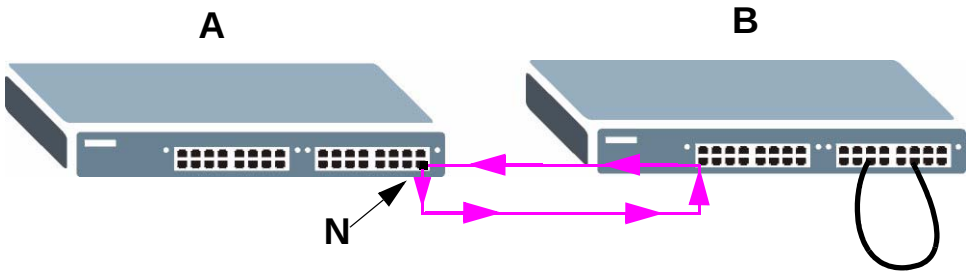
Loop detection is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a MES-2110 that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast frames leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from B.

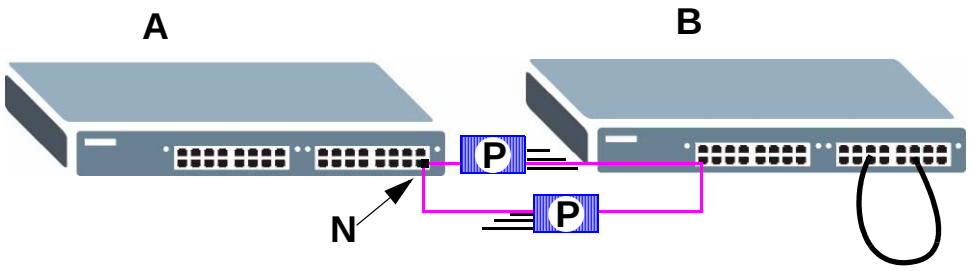
Figure 27 Switch in Loop State



The loop detection feature checks to see if a loop detection enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe frame and seeing if the frame returns on the same port. If this is the case, the MES-2110 will shut down the port connected to the switch in loop state.

The following figure shows a loop detection enabled port **N** on switch **A** sending a probe frame **P** to switch **B**. Since switch **B** is in loop state, the probe frame **P** returns to port **N** on **A**. The MES-2110 then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 28 Loop detection - Probe Frame

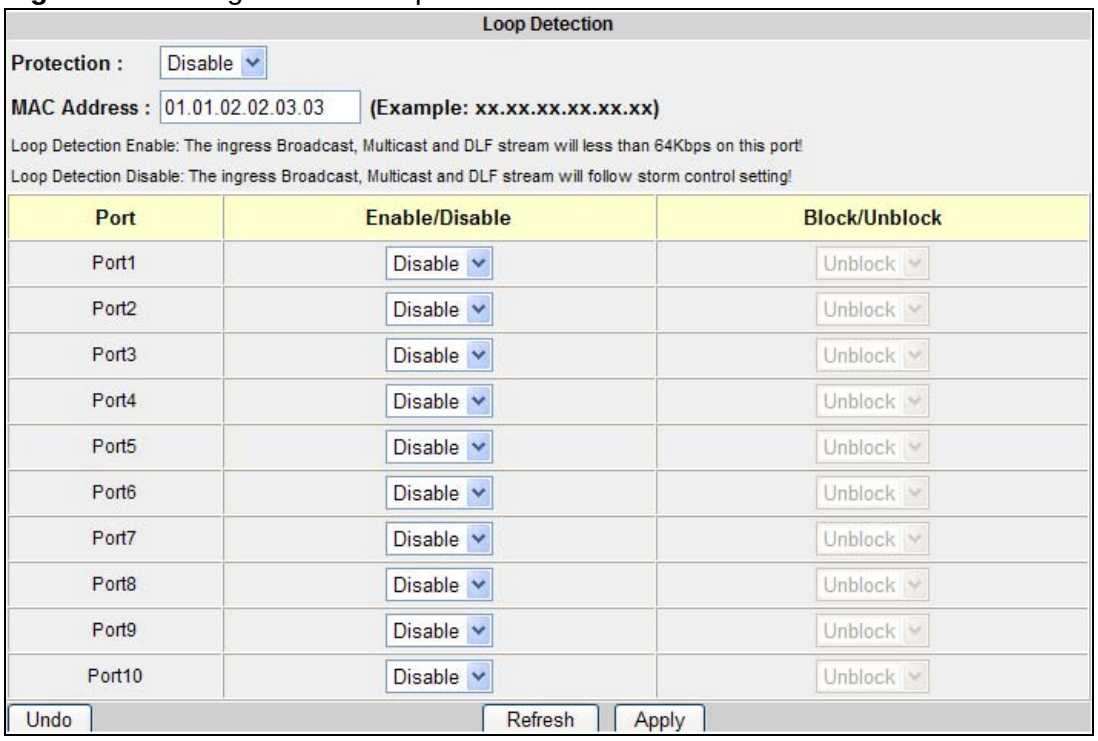


Note: After resolving the loop problem on your network you can re-activate the disabled port via the web configurator or via commands (See the CLI Reference Guide).

8.2 The Loop Detection Screen

Click **Configuration** > **Loop Detection** to open the following screen.

Figure 29 Configuration > Loop Detection



The following table describes the labels in this screen.

Table 13 Configuration > Loop Detection

LABEL	DESCRIPTION
Protection	Select **Enable** or **Disable** to have the MES-2110 apply loop detection. The MES-2110 generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop detection feature.
MAC Address	This is the MAC address of the probe frame sent by the MES-2110. You can configure the field as a unicast or multicast MAC address, depending on your needs. The default MAC address is a multicast address (01.01.02.02.03.03). Some network switch does not forward frames with unrecognized multicast MAC address. Test frames sent out for loop detection will be discarded by this type of switch. Users can configure a unicast MAC address to solve this problem.
Port	This is the port number.
Enable/Disable	Select **Enable** or **Disable** to have the MES-2110 apply loop detection feature on this port. When the loop detection feature is enabled, the MES-2110 sends probe frames from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the MES-2110 will shut down this port.
Block/Unblock	When the MES-2110 detects looping, the system sets the port to **Block**. Use this field to **Unblock** the port once you have manually fixed the loop.
Undo	Click this to restore your last saved settings.
Refresh	Click this to reset the data for the field(s).
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

9

Jumbo Frame

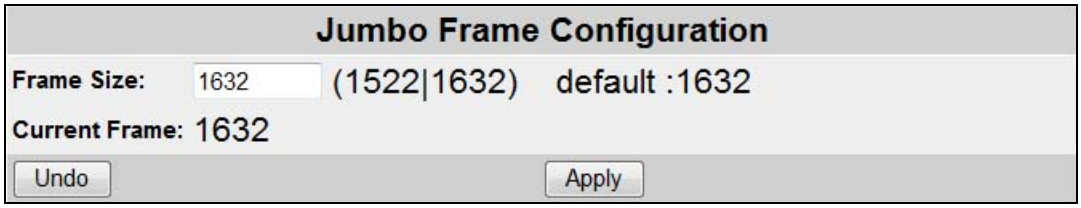
9.1 Overview

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a Gigabit network.

9.2 The Jumbo Frame Configuration Screen

Use this screen to configure the jumbo frame size. Click **Configuration** > **Jumbo Frame** to open the following screen.

Figure 30 Configuration > Jumbo Frame



The following table describes the labels in this screen.

Table 14 Configuration > Jumbo Frame

LABEL	DESCRIPTION
Frame Size	Configure the jumbo frame size (1522 to 1632). The bigger the frame size, the better the performance.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

10

802.1x

10.1 Overview

This chapter describes the IEEE 802.1x authentication method.

Port authentication is a way to validate access to ports on the MES-2110 to clients based on an external server (authentication server). The MES-2110 supports the following method for port authentication:

- **IEEE 802.1x**[1] - An authentication server validates access to a port based on a username and password provided by the user.

IEEE 802.1x authentication uses the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See Section 10.6 on page 84 for more information on configuring your RADIUS server settings.

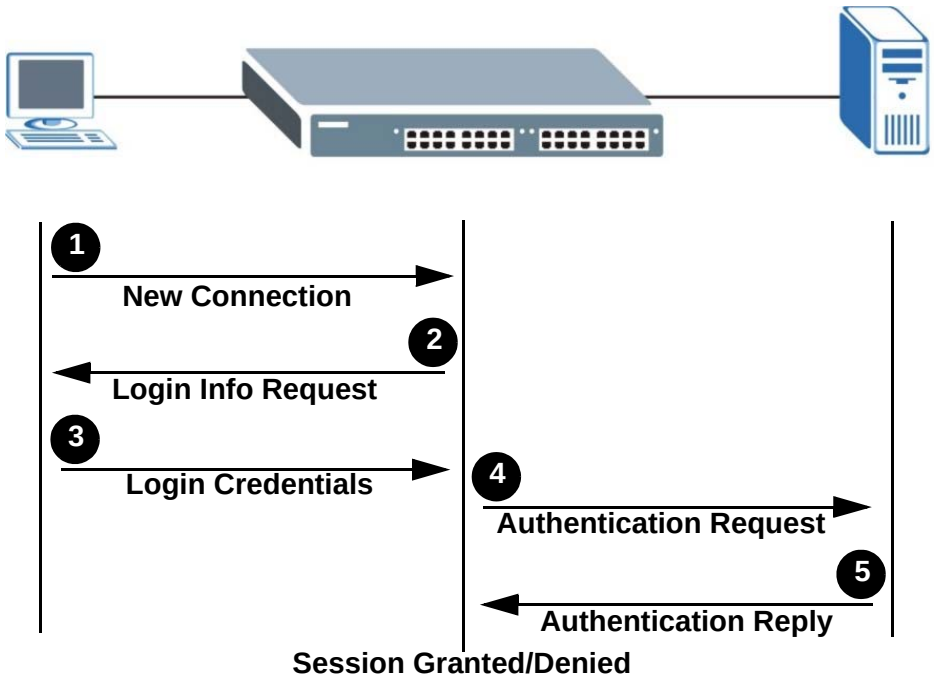
10.1.1 IEEE 802.1x Authentication

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The MES-2110 prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the MES-2110 sends an

1. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Figure 31 IEEE 802.1x Authentication Process



10.1.2 Guest VLAN

When 802.1x port authentication is enabled on the MES-2110, clients that do not have the correct credentials are blocked from using the port(s). You can configure your MES-2110 to have one Guest VLAN. Traffic coming from the Guest VLAN are directed to the Guest network and can have access to unrestricted areas of the network, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the Guest network feature.

Note: Use the MES-2110 to assign the Guest VLAN to a port. This assignment should corresponds to the network's Guest VLAN. The Guest network is not configurable in this MES-2110.

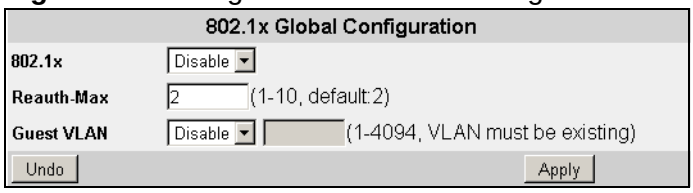
To enable port authentication, first activate the port authentication method (both on the MES-2110 and the port(s)) then configure the RADIUS server settings in the **Radius Server Configuration** screen (Section 10.4 on page 81).

10.2 802.1x Global Configuration Screen

Use this screen to enable port authentication and a guest VLAN on the MES-2110.

Click **Configuration > 802.1x > Global Configuration** in the navigation panel to display the screen as shown.

Figure 32 Configuration > Global Configuration



The following table describes the labels in this screen.

Table 15 Configuration > Global Configuration

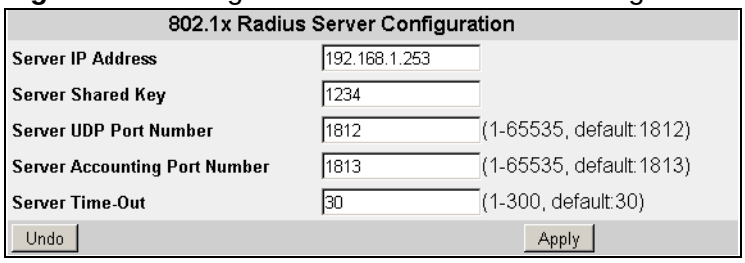
LABEL	DESCRIPTION
802.1x	Select **Enable** to activate the port authentication method on the MES-2110. Otherwise, select **Disable**.
Reauth-Max	Specify the number of times the MES-2110 tries to authenticate client(s) before sending unresponsive ports to the Guest VLAN. This is set to **2** by default. That is, the MES-2110 attempts to authenticate a client twice. If the client does not respond to the first authentication request, the MES-2110 tries again. If the client still does not respond to the second request, the MES-2110 sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the MES-2110 again.
Guest VLAN	Select **Enable** then enter the number that identifies the Guest VLAN. Make sure this is the Guest VLAN recognized in your network. Clients belonging to the guest VLAN can access unprotected areas in your network, such as the Internet. Select **Disable** if you do not want to use this feature.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

10.3 802.1x Radius Server Configuration Screen

Use this screen to configure the RADIUS server settings.

Click **Configuration > 802.1x > Radius Server Configuration** in the navigation panel to display the screen as shown.

Figure 33 Configuration > Radius Server Configuration



The following table describes the labels in this screen.

Table 16 Configuration > Radius Server Configuration

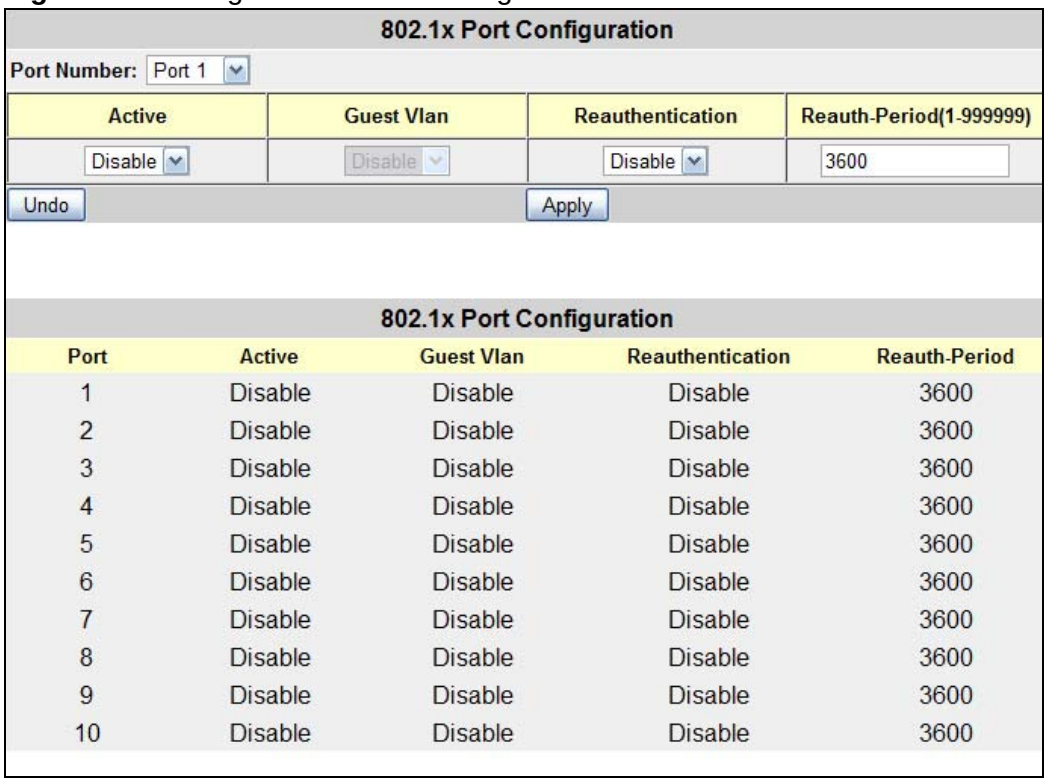
LABEL	DESCRIPTION
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Server Shared Key	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the MES-2110. The key must be the same on the external authentication server and your MES-2110. The key is not sent over the network.
Server UDP Port Number	Enter the port number of the RADIUS server. The default port number is 1812.
Server Accounting Port Number	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Server Time Out	Type how many minutes a session can be left idle before the session times out.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

10.4 802.1x Port Configuration Screen

Use this screen to enable and configure port authentication on individual ports.

Click **Configuration > 802.1x > Port Configuration** in the navigation panel to display the screen as shown.

Figure 34 Configuration > Port Configuration



802.1x Port Configuration

Port Number: Port 1

Active	Guest Vlan	Reauthentication	Reauth-Period(1-999999)
Disable	Disable	Disable	3600

Undo Apply

802.1x Port Configuration

Port	Active	Guest Vlan	Reauthentication	Reauth-Period
1	Disable	Disable	Disable	3600
2	Disable	Disable	Disable	3600
3	Disable	Disable	Disable	3600
4	Disable	Disable	Disable	3600
5	Disable	Disable	Disable	3600
6	Disable	Disable	Disable	3600
7	Disable	Disable	Disable	3600
8	Disable	Disable	Disable	3600
9	Disable	Disable	Disable	3600
10	Disable	Disable	Disable	3600

The following table describes the labels in this screen.

Table 17 Configuration > Port Configuration

LABEL	DESCRIPTION
Port	Select a port number to configure.
Active	Enable this to permit 802.1x authentication on the MES-2110. Note: You must first enable 802.1x authentication on the MES-2110 before configuring it on each port.

Table 17 Configuration > Port Configuration (continued)

LABEL	DESCRIPTION
Guest VLAN	You can configure this if you have enabled the guest VLAN feature in the **Configuration > Global Configuration** screen (see Section 10.2 on page 79). Select **Enable** then enter the number that identifies the Guest VLAN. Make sure this is the Guest VLAN recognized in your network. Clients belonging to the guest VLAN can access unprotected areas in your network, such as the Internet. Select **Disable** if you do not want to use this feature.
Reauthentication	Enable this if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-Period (1-999999)	Specify how often (in minutes) a client has to re-enter his or her username and password to stay connected to the port. Default is **3600** minutes (or 1 hour).
Port	This indicates the port number.
Active	This indicates whether 802.1x authentication is enabled or disabled for this port.
Guest VLAN	This indicates whether **Guest VLAN** is enabled or disabled for this port.
Reauthentication	This indicates whether **Reauthentication** is **enabled** or **disabled** for this port.
Reauth-Period (1-999999)	This indicates the **Reauth-Period** for the this port.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

10.5 802.1x Radius Server Configuration Screen

Use this screen to view a summary of port authentication settings on the MES-2110 and in each individual ports.

Click **Configuration > 802.1x > 802.1x Status** in the navigation panel to display the screen as shown.

Figure 35 Configuration > 802.1x Status

802.1x Status										
802.1x	Disable									
Guest VLAN	Enable									
Reauth-Max	2									
Server IP Address	192.168.1.253									
Server Shared Key	1234									
Sever UDP Port Number	1812									
Server Accounting Port Number	1813									
Sever Time-Out	30									
	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10
	Y:Yes N:No A:Accepted									
Active	N	N	N	N	N	N	N	N	N	N
Guest Vlan	N	N	N	N	N	N	N	N	N	N
Reauthentication	N	N	N	N	N	N	N	N	N	N
Reauth-Period	3600	3600	3600	3600	3600	3600	3600	3600	3600	3600

The following table describes the labels in this screen.

Table 18 Configuration > 802.1x Status

LABEL	DESCRIPTION
802.1x	This shows if port authentication is enabled on the MES-2110.
Guest VLAN	This shows if a Guest VLAN is enabled on the Switch.
Reauth-Max	This shows the number of times the MES-2110 attempts to authenticate clients for port access.
Server IP Address	This is the IP address of the RADIUS server.
Server Shared Key	This is the password shared between the external authentication server and the MES-2110.
Server UDP Port Number	This is the port number of the RADIUS server.
Server Accounting Port Number	This is the port number of the external accounting server.
Server Time-Out	This shows how many minutes a session can be idle before the session times out. When a session times out, the client has to send a new request to the server and be authenticated again.
The table below describes the settings for ports 1-10	
Active	This shows if port authentication is enabled on the port.

Table 18 Configuration > 802.1x Status (continued)

LABEL	DESCRIPTION
Guest VLAN	This shows if a Guest VLAN is enabled on the port.
Reauthentication	This shows if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-Period	This shows how often (in minutes) a client has to re-enter his or her username and password to stay connected to the port.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

10.6 Technical Reference

This section provides technical background information about the topics covered in this chapter.

10.6.1 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 19 RADIUS vs. TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the MES-2110) and the TACACS server is encrypted.

10.6.2 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication, and accounting elements in a user profile, which is stored on the RADIUS server. This appendix lists the RADIUS attributes supported by the MES-2110.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication. Refer to RFC 2866 and RFC 2869 for RADIUS attributes used for accounting.

This section lists the attributes used by authentication and accounting functions on the MES-2110. In cases where the attribute has a specific format associated with it, the format is specified.

10.6.3 Attributes Used for Authentication

The following sections list the attributes sent from the MES-2110 to the RADIUS server when performing authentication.

10.6.3.1 Attributes Used for Authenticating Privilege Access

User-Name

- The format of the User-Name attribute is **$enab#$**, where # is the privilege level (1-14).

User-Password

NAS-Identifier

NAS-IP-Address

10.6.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

10.6.3.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the MES-2110.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

10.6.4 Attributes Used for Accounting

The following sections list the attributes sent from the MES-2110 to the RADIUS server when performing authentication.

10.6.4.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID

- The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 200704191721030000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

10.6.4.2 Attributes Used for Accounting Exec Events

The attributes are listed in the following table along with the time that they are sent (the difference between Console and Telnet/SSH Exec events is that the Telnet/SSH events utilize the Calling-Station-Id attribute):

Table 20 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

Table 21 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Calling-Station-Id	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y

Table 21 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

10.6.4.3 Attributes Used for Accounting IEEE 802.1x Events

The attributes are listed in the following table along with the time of the session they are sent:

Table 22 RADIUS Attributes-Exec Events via 802.1x

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-IP-Address	Y	Y	Y
NAS-Port	Y	Y	Y
Class	Y	Y	Y
Called-Station-Id	Y	Y	Y
Calling-Station-Id	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-Port-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Input-Octets		Y	Y
Acct-Output-Octets		Y	Y
Acct-Session-Time		Y	Y
Acct-Input-Packets		Y	Y
Acct-Output-Packets		Y	Y
Acct-Terminate-Cause			Y
Acct-Input-Gigawords		Y	Y
Acct-Output-Gigawords		Y	Y

11

Bridge

11.1 Overview

The MES-2110 supports Rapid Spanning Tree Protocol (RSTP) as defined in the IEEE 802.1w Rapid Spanning Tree Protocol standard.

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The MES-2110 uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

11.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 23 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535

Table 23 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

11.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network frames are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

11.1.3 STP Port States

STP assigns five port states to eliminate frame looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

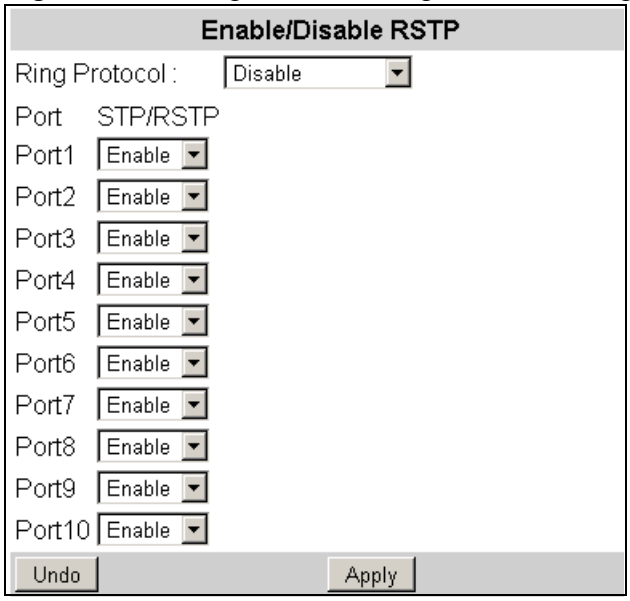
Table 24 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

11.2 The Bridge Configuration Screen

Click **Configuration** > **Bridge Menu** > **Bridge Config** to open the following screen.

Figure 36 Configuration > Bridge Menu > Bridge Config



The following table describes the labels in this screen.

Table 25 Configuration > Bridge Menu > Bridge Config

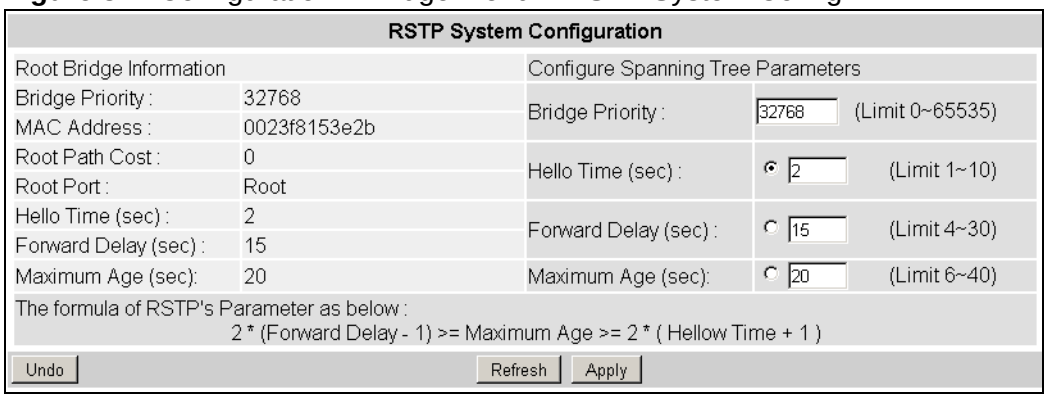
LABEL	DESCRIPTION
Ring Protocol	Select **RSTP (802.1W)** to enable RSTP. Select **Disable** if you do not want to use this feature.
Port	Select **Enable** to have the port participate in RSTP when you select **RSTP (802.1W)** in the **Ring Protocol** field. Select **Disable** so that the port will not participate in RSTP when you select **RSTP (802.1W)** in the Ring Protocol field. Select **Tunnel** so that the port will not participate in RSTP. When the tunnel port receives Bridge Protocol Data Units (BPDU) frames, the MES-2110 forwards the frames to other tunnel ports.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

11.3 The RSTP System Configuration Screen

You must first enable RSTP in the **Bridge Configuration** screen in order to open this screen.

Click **Configuration** > **Bridge Menu** > **RSTP System Config** to open the following screen.

Figure 37 Configuration > Bridge Menu > RSTP System Config


RSTP System Configuration
Root Bridge Information
Bridge Priority : 32768
MAC Address : 0023f8153e2b
Root Path Cost : 0
Root Port : Root
Hello Time (sec) : 2
Forward Delay (sec) : 15
Maximum Age (sec): 20
Configure Spanning Tree Parameters
Bridge Priority : 32768 (Limit 0~65535)
Hello Time (sec) : 2 (Limit 1~10)
Forward Delay (sec) : 15 (Limit 4~30)
Maximum Age (sec): 20 (Limit 6~40)
The formula of RSTP's Parameter as below :
2 * (Forward Delay - 1) >= Maximum Age >= 2 * (Hellow Time + 1)
Undo
Refresh
Apply

The following table describes the labels in this screen.

Table 26 Configuration > Bridge Menu > RSTP System Config

LABEL	DESCRIPTION
Root Bridge Information	
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
MAC Address	This is the root bridge's MAC address.
Root Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 23 on page 89 for more information.
Root Port	This shows whether the MES-2110 connects to another root switch (through port number **1-10**) or serves as a root switch (**Root**).
Hello Time (sec)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Forward Delay (sec)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Max age (sec)	This is the maximum time (in seconds) the MES-2110 can wait without receiving a configuration message before attempting to reconfigure.
Configuration Spanning Tree Parameters	
RSTP Force Version	Use this to force the spanning tree algorithm to run on either the **STP** or **RSTP** protocol.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time (sec)	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

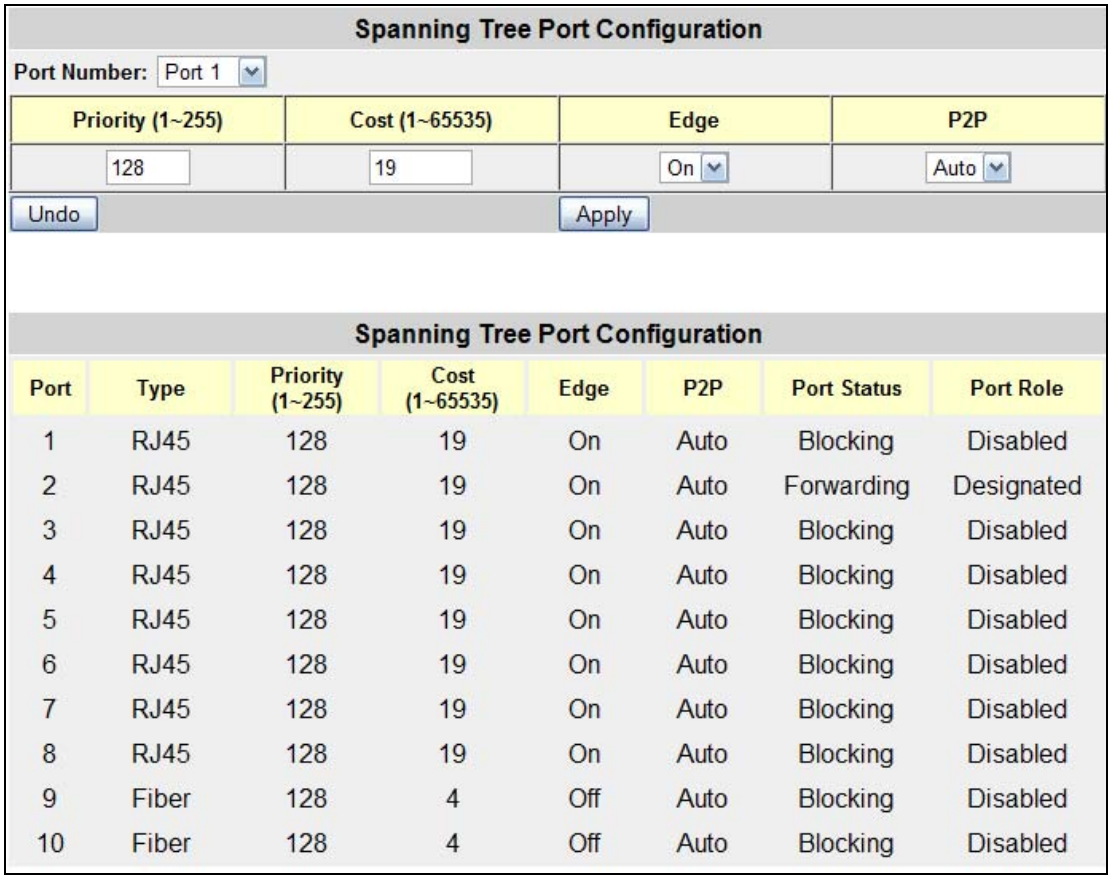
Table 26 Configuration > Bridge Menu > RSTP System Config

LABEL	DESCRIPTION
Forward Delay (sec)	This is the maximum time (in seconds) the MES-2110 will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Max age (sec)	This is the maximum time (in seconds) the MES-2110 can wait without receiving a BPDU before attempting to reconfigure. All MES-2110 ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the MES-2110 ports attached to the network. The allowed range is 6 to 40 seconds.
Undo	Click this to restore your last saved settings.
Refresh	Click this to reset the data for the field(s).
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

11.4 The Spanning Tree Port Configuration

Click **Configuration** > **Bridge Menu** > **RSTP Per Port Config** to open the following screen.

Figure 38 Configuration > Bridge Menu > RSTP Per Port Config



Spanning Tree Port Configuration

Port Number: Port 1

Priority (1~255)	Cost (1~65535)	Edge	P2P
128	19	On	Auto

Undo Apply

Spanning Tree Port Configuration

Port	Type	Priority (1~255)	Cost (1~65535)	Edge	P2P	Port Status	Port Role
1	RJ45	128	19	On	Auto	Blocking	Disabled
2	RJ45	128	19	On	Auto	Forwarding	Designated
3	RJ45	128	19	On	Auto	Blocking	Disabled
4	RJ45	128	19	On	Auto	Blocking	Disabled
5	RJ45	128	19	On	Auto	Blocking	Disabled
6	RJ45	128	19	On	Auto	Blocking	Disabled
7	RJ45	128	19	On	Auto	Blocking	Disabled
8	RJ45	128	19	On	Auto	Blocking	Disabled
9	Fiber	128	4	Off	Auto	Blocking	Disabled
10	Fiber	128	4	Off	Auto	Blocking	Disabled

The following table describes the labels in this screen.

Table 27 Configuration > Bridge Menu > RSTP Per Port Config

LABEL	DESCRIPTION
Port	Select a port to configure.
Priority (1~255)	Enter the port's priority rating. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Cost (1~65535)	Enter the port's path cost. Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 23 on page 89 for more information.

Table 27 Configuration > Bridge Menu > RSTP Per Port Config

LABEL	DESCRIPTION
Edge	Select **On** when the port is connected to an end node (a computer network card for example). Select **Off** when the port is connected to a bridge node.
P2P	Select **On** when the port is connected to one bridge as a Point-to-Point link type. Select **Off** when the port is connected to multiple bridges as a Shared Medium link type. Select **Auto** to have the MES-2110 automatically determine the link type.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Port	This indicates the port index number.
Type	This indicates the cable type connected to the port.
Priority (1~255)	This indicates the port priority.
Cost (1~65535)	This indicates the path cost for the port.
Edge	This indicates whether the port is connected to an end node (**On**) or a bridge node (**Off**).
P2P	This indicates whether the port is connected to one bridge (**On**), multiple bridges (**Off**), or if the connection type is determined automatically (**Auto**).
Port Status	This indicates whether the port is **Forwarding** or **Blocking** frame transmission.
Port Role	This indicates the port behavior as a **Disabled**, **Alternate**, **Backup**, **Root**, **Designated** or **NonStp** port.

12 VLAN

12.1 Overview

This chapter shows you how to configure 802.1Q tagged and port-based VLANs. A VLAN (Virtual Local Area Network) is a network that is not limited by the physical location of a device (such as a switch).

12.2 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

12.2.1 Forwarding Tagged and Untagged Frames

Each port on the MES-2110 is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the MES-2110 first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the MES-2110 first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 28 IEEE 802.1Q VLAN Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the MES-2110 discards incoming frames for VLANs that do not have this port as a member.

12.3 The VLAN Type Screen

Use this screen to select the VLAN type. Click **Configuration** > **VLAN Menu** > **VLAN Type** to open the following screen.

Figure 39 Configuration > VLAN Menu > VLAN Type

The following table describes the labels in this screen.

Table 29 Configuration > VLAN Menu > VLAN Type

LABEL	DESCRIPTION
VLAN Type	Use this to set the MES-2110 to **Port-Based** or **Tag-Based(802.1q)** VLAN mode.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

12.4 The Port-Based VLAN Screen

Port-based VLANs are VLANs where the frame forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data frame leaves) for both ports.

Port-based VLANs are specific only to the MES-2110 on which they were created.

This screen is available only when you select **Port-Based** in the **VLAN Type** screen. Click **Configuration** > **VLAN Menu** > **Port-Based** to open the following screen.

Figure 40 Configuration > VLAN Menu > Port-Based

Port-Based VLAN Configuration

Port Number	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10	Switch Management
Port 1	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Enable

Apply

Port-Based VLAN Status

Port Number	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10	Switch Management
Port1	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Enable
Port2	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Enable
Port3	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Enable
Port4	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Enable
Port5	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Enable
Port6	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Enable
Port7	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Enable
Port8	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Enable
Port9	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Enable
Port10	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Enable

The following table describes the labels in this screen.

Table 30 Configuration > VLAN Menu > Port-Based

LABEL	DESCRIPTION
Port-Based VLAN Configuration	
Port Number	Use this to select the port you are configuring.
Port1-10	Select the subscriber ports that can talk to each other.
Switch Management	Use this to enable or disable switch management via the web configurator, Telnet or SNMP manager. Select the port through which you can manage the MES-2110. If you disable this feature, then you cannot access the web configurator from a computer connected to this port.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Port-Based VLAN Status	
Port Number	This is the port number.
Port1-10	This shows the subscriber ports that can talk to each other.
Switch Management	This shows whether switch management is enabled or disabled.

12.5 The Tag-Based VLAN Screens

Use the **Tag-Based VLAN** screens to configure VLAN settings.

12.5.1 VLAN Stacking

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

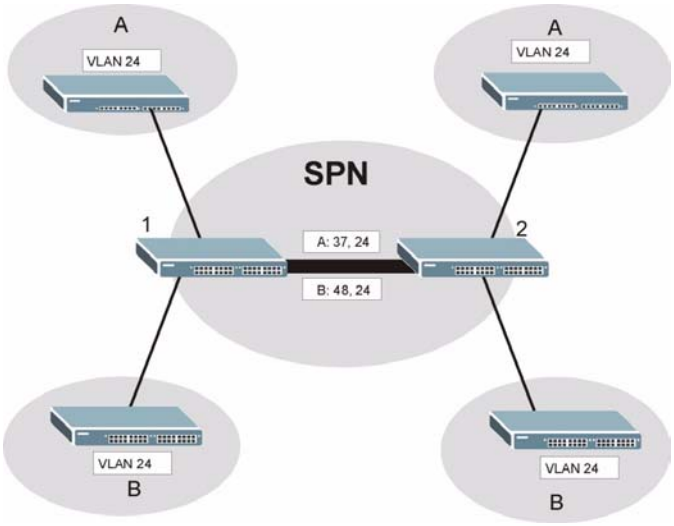
A service provider’s customers may require a range of VLANs to handle multiple applications. A service provider’s customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

12.5.2 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider’s Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to

distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 41 VLAN Stacking Example



12.5.3 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel** (the latter is for Gigabit ports only).

Note: Some devices do not support all roles.

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.

Note: Static VLAN **Tx Tagging** MUST be disabled on a port where you choose **Normal** or **Access Port**.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

Note: Static VLAN **Tx Tagging** MUST be enabled on a port where you choose **Tunnel Port**.

12.5.4 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 31 VLAN Tag Format

Type	Priority	VID

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access**, then the MES-2110 adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel**, then the MES-2110 only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the MES-2110. (If an incoming frame's **SP TPID** is the same as the one configured on the MES-2110, then the MES-2110 will not add the tag.)

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the MES-2110, configure priority level of inner IEEE 802.1Q tag in the **Configuration** > **QoS Menu** > **802.1p Priority** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

12.5.5 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a “double-tagged” 802.1Q frame (service provider) is shown next.

Configure the fields as highlighted in the MES-2110 **VLAN Stacking** screen.

Table 32 Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/ Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	**SPTPID**	**Priority**	**VID**	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	Double-tagged frame

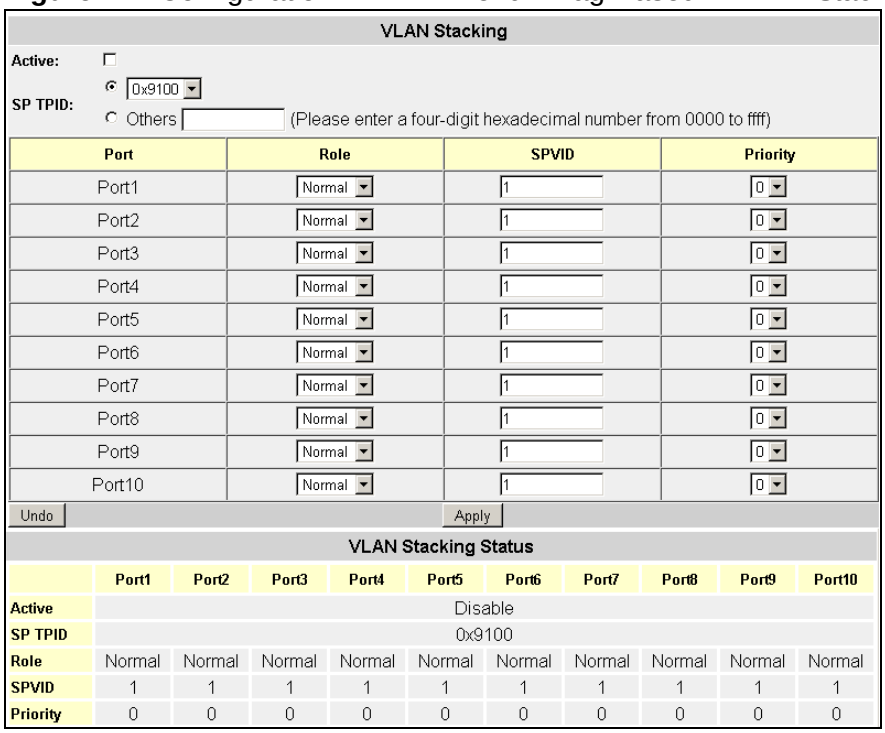
Table 33 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/ Etype	Length and type of Ethernet frame
(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

12.5.6 The VLAN Stacking Configuration Screen

Use this screen to enable VLAN stacking on the MES-2110. Click **Configuration** > **VLAN Menu** > **Tag-Based** > **VLAN Stacking** to open the following screen.

Figure 42 Configuration > VLAN Menu > Tag-Based > VLAN Stacking



The following table describes the labels in this screen.

Table 34 Configuration > VLAN Menu > Tag-Based > VLAN Stacking

LABEL	DESCRIPTION
VLAN Stacking	
Active	Select this to enable VLAN stacking on the MES-2110.
SP TPID	**SP TPID** is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Choose **0x8100** or **0x9100** from the drop-down list box or select **Others** and then enter a four-digit hexadecimal number from 0x0000 to 0xFFFF. 0x denotes a hexadecimal number. It does not have to be typed in the **Others** text field.
Port	The port number identifies the port you are configuring.
Role	Select **Access** to have the MES-2110 add the **SP TPID** tag to all incoming frames received on this port. Select **Access Port** for ingress ports at the edge of the service provider's network. Select **Tunnel** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.

Table 34 Configuration > VLAN Menu > Tag-Based > VLAN Stacking

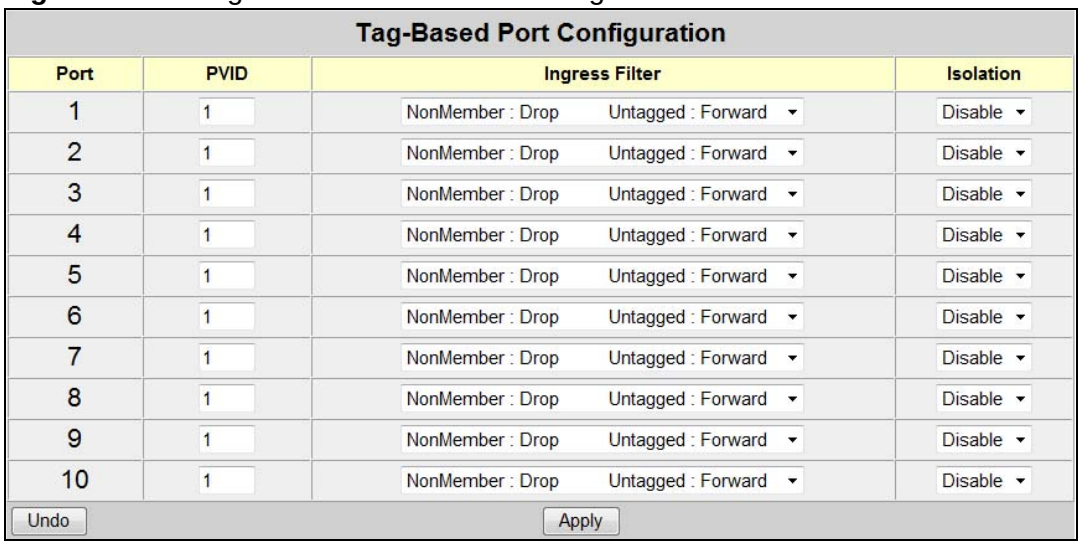
LABEL	DESCRIPTION
SPVID	**SPVID** is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port.
Priority	On the MES-2110, configure priority level of inner IEEE 802.1Q tag in the **Configuration** > **QoS Menu** > **802.1p Priority** screen. "0" is the lowest priority level and "7" is the highest.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
VLAN Stacking Status	
Port1-10	This is the port number.
Active	This shows whether VLAN stacking is enabled or disabled on the MES-2110.
SP TPID	This is the service provider VLAN tag.
Role	This shows how the port process transmitted frames.
SPVID	This is the service provider ID for frames received on this port.
Priority	This shows the priority level of frames transmitted through the port.

12.5.7 The Tag-Based Port Information Screen

Use this screen to configure how the MES-2110 handles incoming traffic passing through the port.

Click **Configuration** > **VLAN Menu** > **Tag-Based** > **Port Info.** to open the following screen.

Figure 43 Configuration > VLAN Menu > Tag-Based > Port Info.


Tag-Based Port Configuration
Port
PVID
Ingress Filter
Isolation
1 1 NonMember : Drop Untagged : Forward Disable
2 1 NonMember : Drop Untagged : Forward Disable
3 1 NonMember : Drop Untagged : Forward Disable
4 1 NonMember : Drop Untagged : Forward Disable
5 1 NonMember : Drop Untagged : Forward Disable
6 1 NonMember : Drop Untagged : Forward Disable
7 1 NonMember : Drop Untagged : Forward Disable
8 1 NonMember : Drop Untagged : Forward Disable
9 1 NonMember : Drop Untagged : Forward Disable
10 1 NonMember : Drop Untagged : Forward Disable
Undo
Apply

The following table describes the labels in this screen.

Table 35 Configuration > VLAN Menu > Tag-Based > Port Info.

LABEL	DESCRIPTION
Port	This is the port index number.
PVID	Enter a number between 1 and 4094 as the port VLAN ID.
Ingress Filter	Use this to determine the action about incoming traffic passing through the port. • **NonMember: Forward, Untagged: Forward**: Forward frames that do not belong to any VLAN group and forward untagged VLAN frames. • **NonMember: Drop, Untagged: Forward**: Drop frames that do not belong to any VLAN group and forward untagged VLAN frames. • **NonMember: Drop, Untagged: Drop**: Drop frames that do not belong to any VLAN group and drop untagged VLAN frames.
Isolation	Use this to enable or disable port isolation. Port isolation allows each port to communicate only with the management port but not communicate with each other. This option is the most limiting but also the most secure.

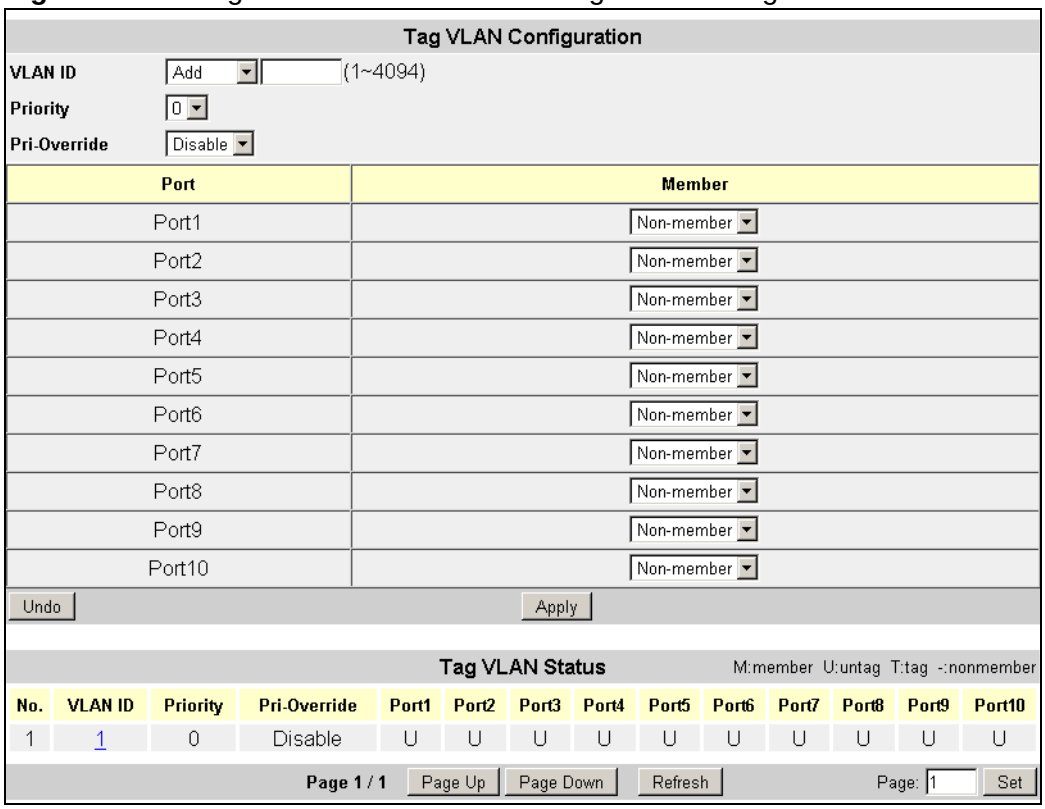
Table 35 Configuration > VLAN Menu > Tag-Based > Port Info.

LABEL	DESCRIPTION
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

12.5.8 The Tag-Based Port Configuration Screen

Use this screen to configure the VLAN group settings for each port on the MES-2110. Click **Configuration** > **VLAN Menu** > **Tag-Based** > **Tag-Based info.** to open the following screen.

Figure 44 Configuration > VLAN Menu > Tag-Based > Tag-Based info.



The following table describes the labels in this screen.

Table 36 Configuration > VLAN Menu > Tag-Based > Tag-Based info.

LABEL	DESCRIPTION
VLAN ID	Select whether you want to **Add** or **Modify** a VLAN ID. Enter the VLAN ID from 1-4094 that you want to configure.
Priority	This is the priority you want to assign to the tag-based VLAN.

Table 36 Configuration > VLAN Menu > Tag-Based > Tag-Based info.

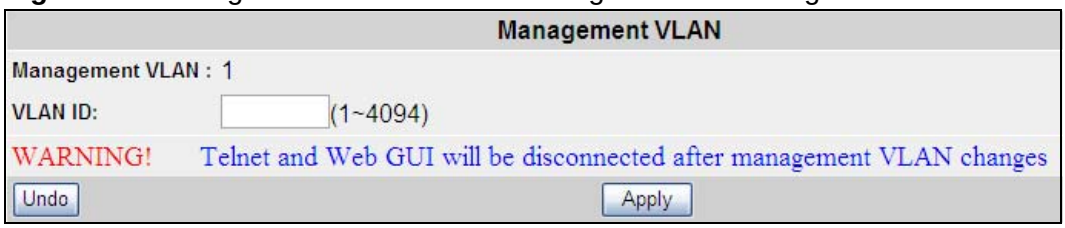
LABEL	DESCRIPTION
Pri-Override	Select **Enable** to ignore the priority level assigned to the transmitted frames. Otherwise, select **Disable**.
Port	This shows ports 1 to 10.
Member	This shows the VLAN group setting for the port, whether it is a **Member**, **Untagging**, **Tagging** or **Non-member**.
Undo	Click this to reset the values in this screen to their last-saved values.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Tag VLAN Status (M:member U:untag T:tag)	
Add VLAN Configuration	
VLAN ID	Enter a VLAN ID number from 1 to 4094.
Priority	This is the priority you want to assign to the Tag-based VLAN.
Pri-Override	Select **Enable** to ignore the priority level assigned to the transmitted frames. Otherwise, select **Disable**.
Port 1-10	A **Member** port is a permanent member of this VLAN group. An **Untagging** port strips off the 802.1Q tag from incoming and outgoing frames. Use this to send untag frames to devices that do no support the 802.1Q feature. A **Tagging** port tags incoming and outgoing frames with this VLAN group information. A **Non-member** port does not participate in the VLAN group.
Page Up	Click this to view the next page.
Page Down	Click this to view the previous page.
Refresh	Click this to refresh the screen.
Page... Set	Enter a page number and click Set to go to that page.

12.5.9 The Management VLAN Screen

Use this to configure the management VLAN. A port must belong to the management VLAN if you want to access the MES-2110's web configurator via that

port. Click **Configuration** > **VLAN Menu** > **Tag-Based** > **Management VLAN** to open the following screen.

Figure 45 Configuration > VLAN Menu > Tag-Based > Management VLAN



The following table describes the labels in this screen.

Table 37 Configuration > VLAN Menu > Tag-Based > Management VLAN

LABEL	DESCRIPTION
Management VLAN	This is the current management VLAN.
VLAN ID	Enter an ID number from 1 to 4094. 1 is the default value. If you change this, you will be disconnected from the web configurator unless your current access belongs to the new VLAN.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

13

Bandwidth Control

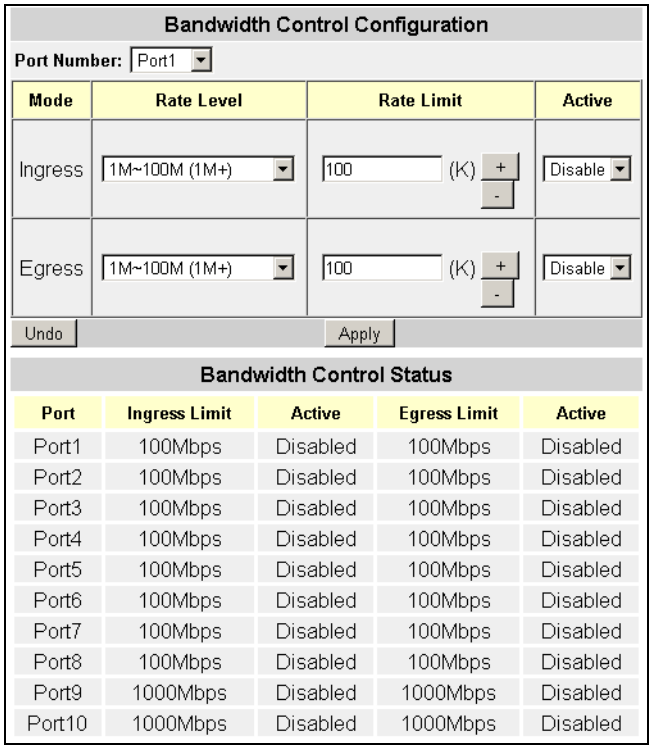
13.1 Overview

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

13.2 Bandwidth Control Setup

Click **Configuration** > **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 46 Configuration > Bandwidth Control



Bandwidth Control Configuration

Port Number: Port1

Mode	Rate Level	Rate Limit	Active
Ingress	1M~100M (1M+)	100 (K) + -	Disable
Egress	1M~100M (1M+)	100 (K) + -	Disable

Undo Apply

Bandwidth Control Status

Port	Ingress Limit	Active	Egress Limit	Active
Port1	100Mbps	Disabled	100Mbps	Disabled
Port2	100Mbps	Disabled	100Mbps	Disabled
Port3	100Mbps	Disabled	100Mbps	Disabled
Port4	100Mbps	Disabled	100Mbps	Disabled
Port5	100Mbps	Disabled	100Mbps	Disabled
Port6	100Mbps	Disabled	100Mbps	Disabled
Port7	100Mbps	Disabled	100Mbps	Disabled
Port8	100Mbps	Disabled	100Mbps	Disabled
Port9	1000Mbps	Disabled	1000Mbps	Disabled
Port10	1000Mbps	Disabled	1000Mbps	Disabled

The following table describes the related labels in this screen.

Table 38 Configuration > Bandwidth Control

LABEL	DESCRIPTION
Bandwidth Control Configuration	
Port Number	Use this to select a port number.
Mode	This shows the **Ingress** (incoming) or **Egress** (outgoing) mode.
Rate Level	Select a rate range from the list. Options are: 64K~960K (64+), 1M~100M (1M+), 110M~1000M (10M+).
Rate Limit	Specify the maximum bandwidth allowed for the traffic flow on a port. The unit changes depending on how you configure in the **Rate Level** field. The value you enter in this field must be within the rate level range.
Active	Use this to enable or disable bandwidth control.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Bandwidth Control Status	
Port	This is the port number.
Ingress Limit	This is the ingress rate limit on the port.
Active	This shows whether bandwidth control for ingress traffic is enabled or disabled on the port.
Egress Limit	This is the egress rate limit on the port.
Active	This shows whether bandwidth control for egress traffic is enabled or disabled on the port.

14

Broadcast Storm Control

14.1 Overview

This chapter introduces and shows you how to configure the broadcast storm control feature.

14.2 Broadcast Storm Control Setup

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) frames the MES-2110 receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF frames is reached per second, the subsequent frames are discarded. Enable this feature to reduce broadcast, multicast and/or DLF frames in your network. You can specify limits for each frame type on each port.

Click **Configuration** > **Storm Control** in the navigation panel to display the screen as shown next.

Figure 47 Configuration > Storm Control

Storm Control Configuration

Port Number: Port1

Mode	Rate Level	Rate Limit	Active
Broadcast	1M~100M (1M+)	100 (K) + -	Disable

Undo Apply

Storm Control Status

Port	Broadcast Limit	Active	Multicast Limit	Active	DLF Limit	Active
Port1	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port2	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port3	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port4	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port5	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port6	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port7	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port8	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port9	1000Mbps	Disabled	1000Mbps	Disabled	1000Mbps	Disabled
Port10	1000Mbps	Disabled	1000Mbps	Disabled	1000Mbps	Disabled

The following table describes the labels in this screen.

Table 39 Configuration > Storm Control

LABEL	DESCRIPTION
Storm Control Configuration	
Port Number	Use this to select a port number.
Mode	Select the **Broadcast**, **Multicast** or **DLF** mode from the list.
Rate Level	Select a rate range from the list. Options are: 64K~960K (64+), 1M~100M (1M+), 110M~1000M (10M+).
Rate Limit	Specify specify how many frames the port receives per second. The unit changes depending on how you configure in the **Rate Level** field. The value you enter in this field must be within the rate level range.
Active	Use this to enable or disable storm control.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Storm Control Status	
Port	This is the port number.
Broadcast Limit	This is the broadcast frame limit on the port.
Active	This shows whether broadcast control is enabled or disabled on the port.
Multicast Limit	This is the multicast frame limit on the port.
Active	This shows whether multicast control is enabled or disabled on the port.
DLF Limit	This is the Destination Lookup Failure (DLF) frame limit on the port.
Active	This shows whether DLF control is enabled or disabled on the port.

15

Port Mirroring

15.1 Overview

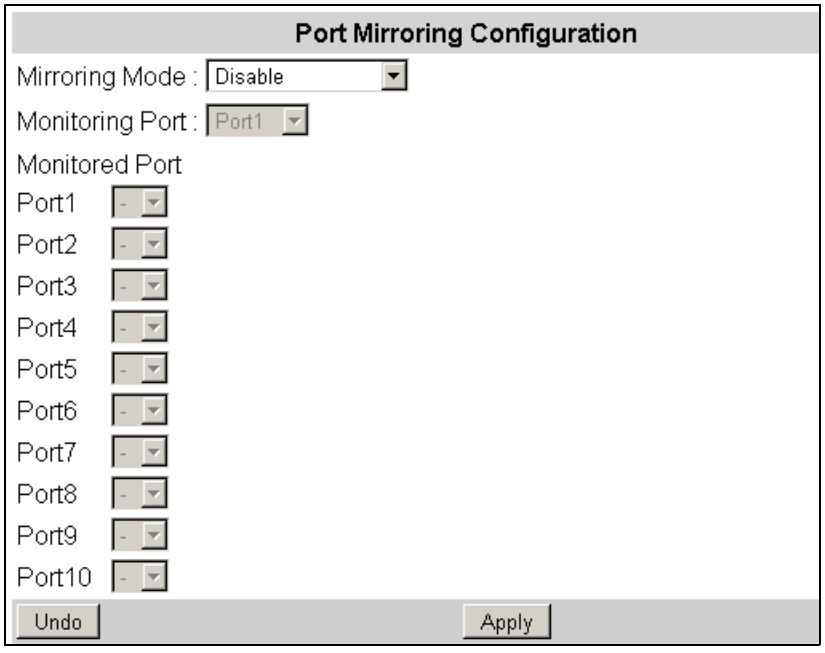
This chapter discusses port mirroring setup screens.

15.2 Port Mirroring Setup

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

Click **Configuration > Port Mirroring** in the navigation panel to display the following screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 48 Configuration > Port Mirroring



The following table describes the labels in this screen.

Table 40 Configuration > Port Mirroring

LABEL	DESCRIPTION
Mirroring Mode	Use this to enable or disable the port mirroring feature. The active port mirroring feature monitors both incoming and outgoing traffic.
Monitoring Port	The monitoring port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select the monitor port number from the list.
Monitored Port	Select the port(s) to mirror the traffic on a port.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

16

Link Aggregation

16.1 Overview

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

The MES-2110 supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your MES-2110.

See Section 16.3 on page 118 for a static port trunking example.

16.2 Dynamic Link Aggregation

The MES-2110 adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The MES-2110 supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregation Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

16.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information[2]:

Table 41 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Table 42 Link Aggregation ID: Peer Switch

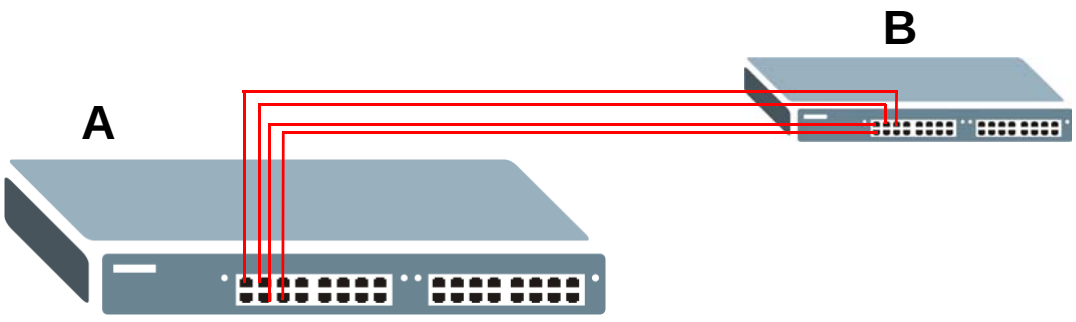
SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

16.3 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

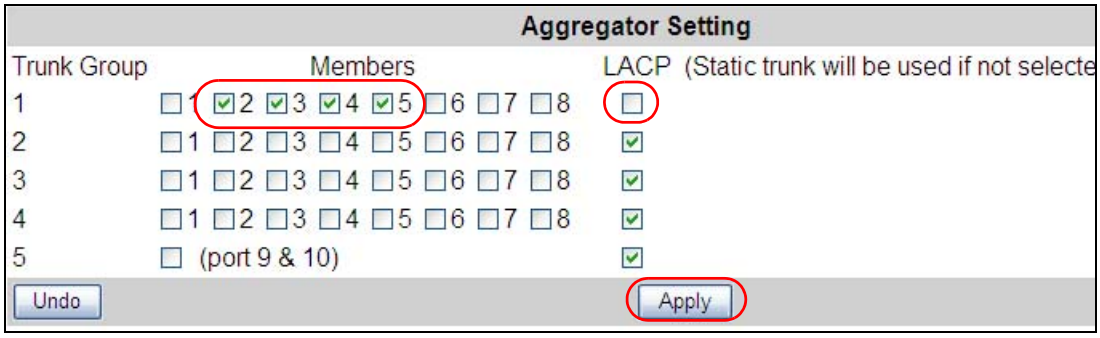
Figure 49 Trunking Example - Physical Connections



2. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

2 **Configure static trunking**-Click **Configuration** > **Trunk Config** > **Aggregator Setting**. In this screen select the ports that should belong to trunk group 1 as shown in the figure below. Do not select the **LACP** option. Click **Apply** when you are done.

Figure 50 Trunking Example - Configuration Screen

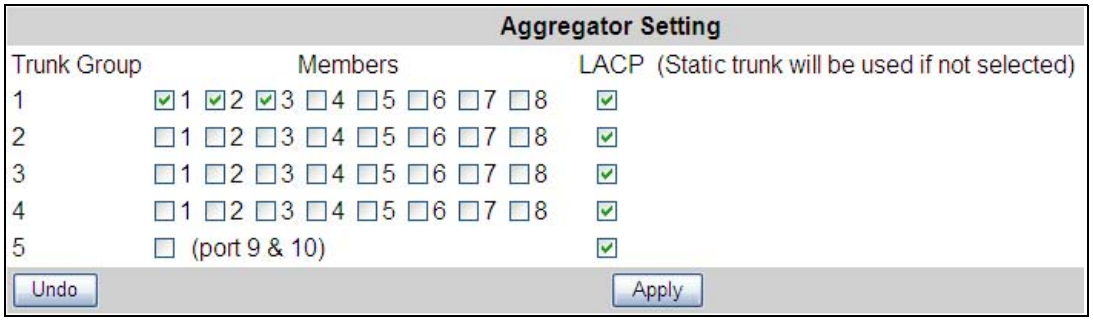

Aggregator Setting
Trunk Group
Members
LACP (Static trunk will be used if not selecte
1 1 2 3 4 5 6 7 8
2 1 2 3 4 5 6 7 8
3 1 2 3 4 5 6 7 8
4 1 2 3 4 5 6 7 8
5 (port 9 & 10)
Undo
Apply

Your trunk group 1 configuration is now complete; you do not need to go to any additional screens.

16.4 Link Aggregation Setting

Click **Configuration** > **Trunk Config > Aggregator Setting** to display the screen shown next. See Section 16.1 on page 117 for more information on link aggregation.

Figure 51 Configuration > Trunk Config > Aggregator Setting


Aggregator Setting
Trunk Group
Members
LACP (Static trunk will be used if not selected)
1 1 2 3 4 5 6 7 8
2 1 2 3 4 5 6 7 8
3 1 2 3 4 5 6 7 8
4 1 2 3 4 5 6 7 8
5 (port 9 & 10)
Undo
Apply

The following table describes the labels in this screen.

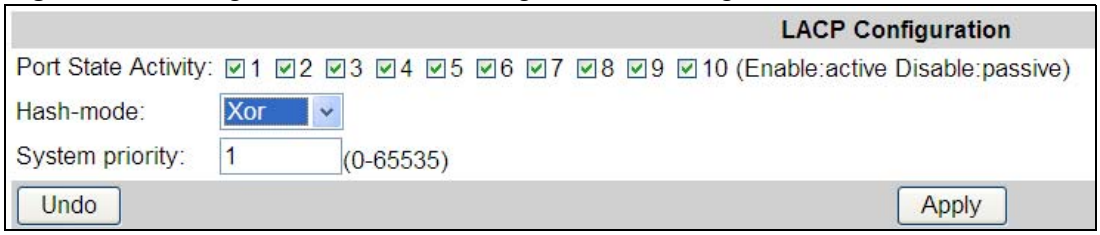
Table 43 Configuration > Trunk Config > Aggregator Setting

LABEL	DESCRIPTION
Group	This is the trunk group index number. The MES-2110 supports up to four trunk groups for 100Mbps ports and up to two trunk groups for Gigabit ports. 100Mbps ports and Gigabit ports cannot be in the same group.
Members	Select the port(s) that belong to a trunk group. For Groups 1 to 4, you can select up to four port members for each group. For Group 5, you can select the two Gigabit ports as the members.
LACP	Use this to enable or disable LACP port trunking.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

16.5 Link Aggregation Control Protocol

Click **Configuration** > **Trunk Config** > **LACP Configuration** to display the screen shown next. See Section 16.2 on page 117 for more information on dynamic link aggregation.

Figure 52 Configuration > Trunk Config > LACP Configuration


LACP Configuration
Port State Activity: 1 2 3 4 5 6 7 8 9 10 (Enable:active Disable:passive)
Hash-mode: Xor
System priority: 1 (0-65535)
Undo
Apply

The following table describes the labels in this screen.

Table 44 Configuration > Trunk Config > LACP Configuration

LABEL	DESCRIPTION
Port State Activity	Select the port to enable Link Aggregation Control Protocol (LACP).
Hash-mode	Use this to specify the outgoing traffic distribution type. Select **Lookup** to distribute frames based on the destination MAC address. Select **Xor** to distribute frames based on the last 3 bits of the source MAC address and the trunk mask load balancing table.

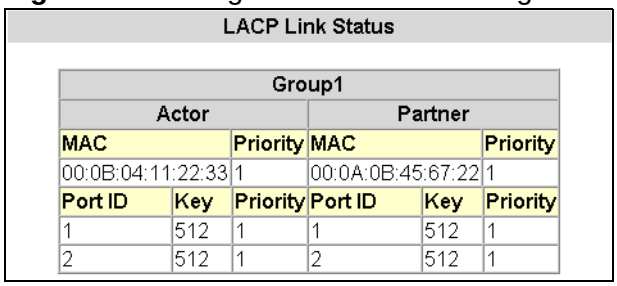
Table 44 Configuration > Trunk Config > LACP Configuration (continued)

LABEL	DESCRIPTION
System Priority	LACP system priority is a number between 1 and 65535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.

16.6 LACP Link Status

Click **Configuration** > **Trunk Config > LACP Link Status** in the navigation panel to open the following screen.

Figure 53 Configuration > Trunk Config > LACP Link Status


LACP Link Status

Group1					
Actor			Partner		
MAC		Priority	MAC		Priority
00:0B:04:11:22:33		1	00:0A:0B:45:67:22		1
Port ID	Key	Priority	Port ID	Key	Priority
1	512	1	1	512	1
2	512	1	2	512	1

The following table describes the labels in this screen.

Table 45 Configuration > Trunk Config > LACP Link Status

LABEL	DESCRIPTION
Actor	This is the local MES-2110.
MAC	This is the local MES-2110's MAC address.
Priority	This is the local MES-2110's priority level.
Port ID	This shows the port number belonging to the trunk group.
Key	This is the local MES-2110's key value.
Priority	This is the port priority level.
Partner	This is the peer MES-2110.
MAC	This is the peer MES-2110's MAC address.
Priority	This is the peer MES-2110's priority level.
Port ID	This shows the port number belonging to the trunk group.

Table 45 Configuration > Trunk Config > LACP Link Status (continued)

LABEL	DESCRIPTION
Key	This is the peer MES-2110's key value.
Priority	This is the port priority level.

17 IGMP

17.1 Overview

Traditionally, IP frames are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP frames to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

17.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send frames to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

17.1.2 IGMP Snooping

A MES-2110 can passively snoop on IGMP frames transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP frames passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the MES-2110 to learn multicast groups without you having to manually configure them.

The MES-2110 forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your MES-2110.

17.1.3 IGMP Snooping and VLANs

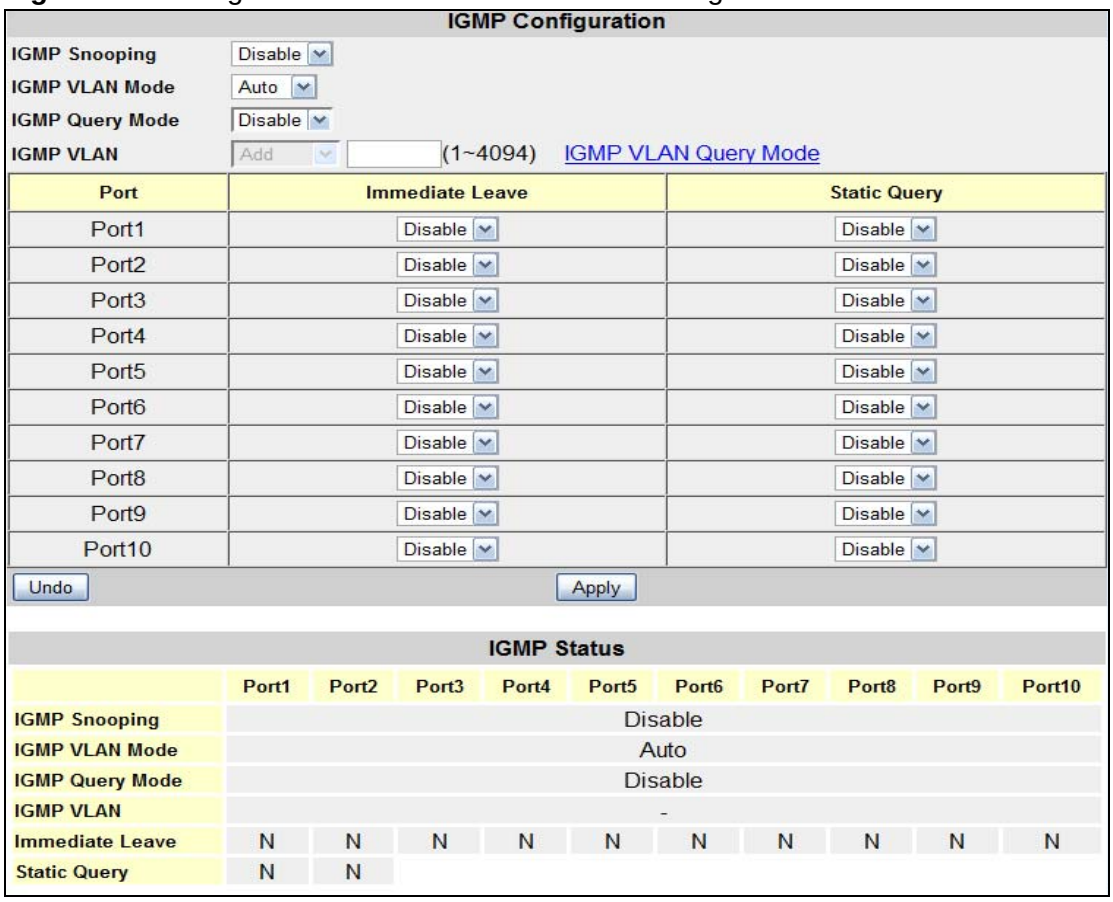
The MES-2110 can perform IGMP snooping on up to 16 VLANs. You can configure the MES-2110 to automatically learn multicast group membership of any VLANs. The MES-2110 then performs IGMP snooping on the first 16 VLANs that send IGMP frames. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the MES-2110 does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

17.2 IGMP Configuration

Use this screen to configure the MES-2110's IGMP settings.

Click **Configuration** > **IGMP Menu** > **IGMP Config** to open the following screen.

Figure 54 Configuration > IGMP Menu > IGMP Config



The following table describes the labels in this screen.

Table 46 Configuration > IGMP Menu > IGMP Config

LABEL	DESCRIPTION
IGMP Snooping	Use this to enable or disable IGMP snooping. When IGMP is enabled, the MES-2110 forwards group multicast traffic only to ports that are members of that group.
IGMP VLAN Mode	Select **Auto** to have the MES-2110 learn multicast group membership information of any VLANs automatically. Select **Fixed** to have the MES-2110 only learn multicast group membership information of the VLAN(s) that you specify below.
IGMP Query Mode	Specifies whether or not the port is an IGMP query port. The MES-2110 forwards IGMP join or leave frames to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. Select **Auto** to have the MES-2110 use the port as an IGMP query port if the port received IGMP query frames recently. An auto port doesn't forward any multicast group member information to its uplink router if the switch didn't receive any IGMP query frames from the router within a period. Select **Disable** to turn this feature off for this port.
IGMP VLAN	Enter the ID of the static VLAN(s) that the MES-2110 includes in its learning process of multicast group membership (of the ports). Enter a VLAN ID between 1 and 4094.
IGMP VLAN Query Mode	Click this to display the **IGMP VLAN Query Mode** screen.
Port 1-10	This shows the port numbers that you can configure individually using the fields described below. The Switch can forward multicast frames to IGMP static ports with or without the learning process of multicast group membership.
Immediate Leave	Use this to enable or disable this feature. When this is enabled on this port and the switch receives an IGMP version 2 leave message for this port, this port is immediately removed from the multicast group. When this is disabled on this port and the switch receives an IGMP version 2 leave message for this port, the Switch first uses this port to send a query packet to ask its multicast group if it still has active client requests. After one second and the Switch has not receive a reply packet asking for the port's IGMP report, it removes the port from the multicast group.
Static Query	Select **Enable** to stop the MES-2110 from using the port as an IGMP query port. The MES-2110 will not keep any record of an IGMP router being connected to this port. Select **Disable** to have the MES-2110 use the port as an IGMP query port if the port receives IGMP query frames.
Undo	Click this to restore your last saved settings.

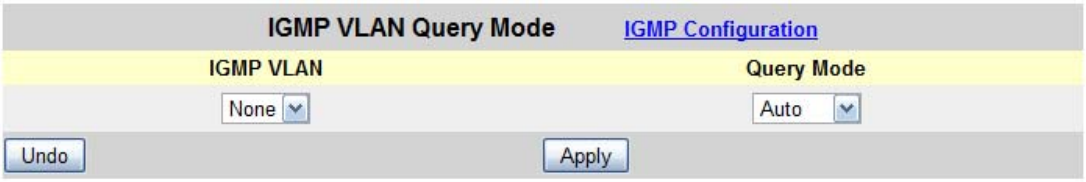
Table 46 Configuration > IGMP Menu > IGMP Config

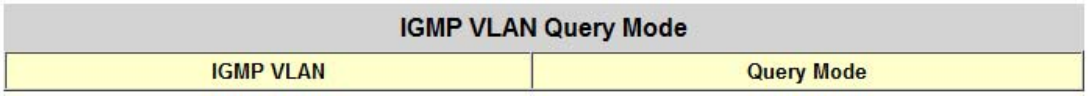
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
IGMP Snooping	This indicates whether IGMP snooping is enabled or disabled for this port.
IGMP VLAN Mode	This indicates whether the IGMP VLAN Mode is set to **Auto** or **Fixed** for this port.
IGMP Query Mode	This indicates whether the IGMP Query Mode is set to **Auto** or **Disable** for this port.
IGMP VLAN	This indicates the static VLAN ID the MES-2110 uses to learn multicast group membership.
Immediate Leave	This indicates whether **Immediate Leave** is enabled or disabled for this port.
Static Query	This indicates whether **Static Query** is enabled or disabled for this port.

17.2.1 IGMP VLAN Query Mode

Click **Configuration** > **IGMP Menu** > **IGMP Config** then click the **IGMP VLAN Query Mode** link to open the following screen.

Figure 55 Configuration > IGMP Menu > IGMP VLAN Query Mode





The following table describes the labels in this screen.

Table 47 Configuration > IGMP Menu > IGMP VLAN Query Mode

LABEL	DESCRIPTION
IGMP VLAN	Select an IGMP VLAN (previously configured in Section 17.2 on page 124) from the list.
Query Mode	Select either **Auto** or **Disable** as the Query Mode for the specified IGMP VLAN.
Undo	Click this to restore your last saved settings.

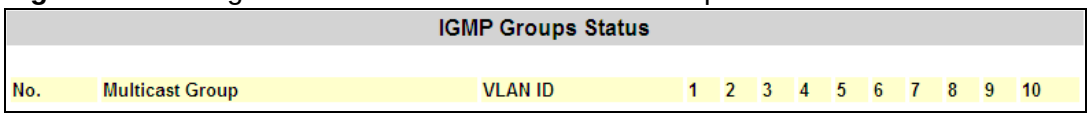
Table 47 Configuration > IGMP Menu > IGMP VLAN Query Mode (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
IGMP VLAN	This column displays the configured VLANs.
Query Mode	This column displays the whether the VLAN's query mode is **Auto** or **Disable**.

17.3 IGMP Status

Click **Configuration > IGMP Menu** > **IGMP Group Status** to display the screen as shown. This screen shows the multicast group information. See Section 17.1 on page 123 for more information on multicasting.

Figure 56 Configuration > IGMP Menu > IGMP Group Status



The following table describes the labels in this screen.

Table 48 Configuration > IGMP Menu > IGMP Group Status

LABEL	DESCRIPTION
No	This is the index number of the entry.
Multicast Group	This field displays IP multicast group addresses.
VLAN ID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.

17.4 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the MES-2110 and **S**.

Figure 57 MVR Network Example

17.4.1 Types of MVR Ports

In MVR, a source port is a port on the MES-2110 that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the MES-2110 maintains a forwarding table that matches the multicast stream to the associated multicast group.

17.4.2 MVR Modes

You can set your MES-2110 to operate in either dynamic or compatible mode.

In dynamic mode, the MES-2110 sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the MES-2110 does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

17.4.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the MES-2110. Multiple subscriber devices can connect through a port configured as the receiver on the MES-2110.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the MES-2110 to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the MES-2110,

an entry is created in the forwarding table on the MES-2110. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the MES-2110 to leave the multicast group. The MES-2110 sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the MES-2110). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the MES-2110 removes the receiver port from the forwarding table.

Figure 58 MVR Multicast Television Example

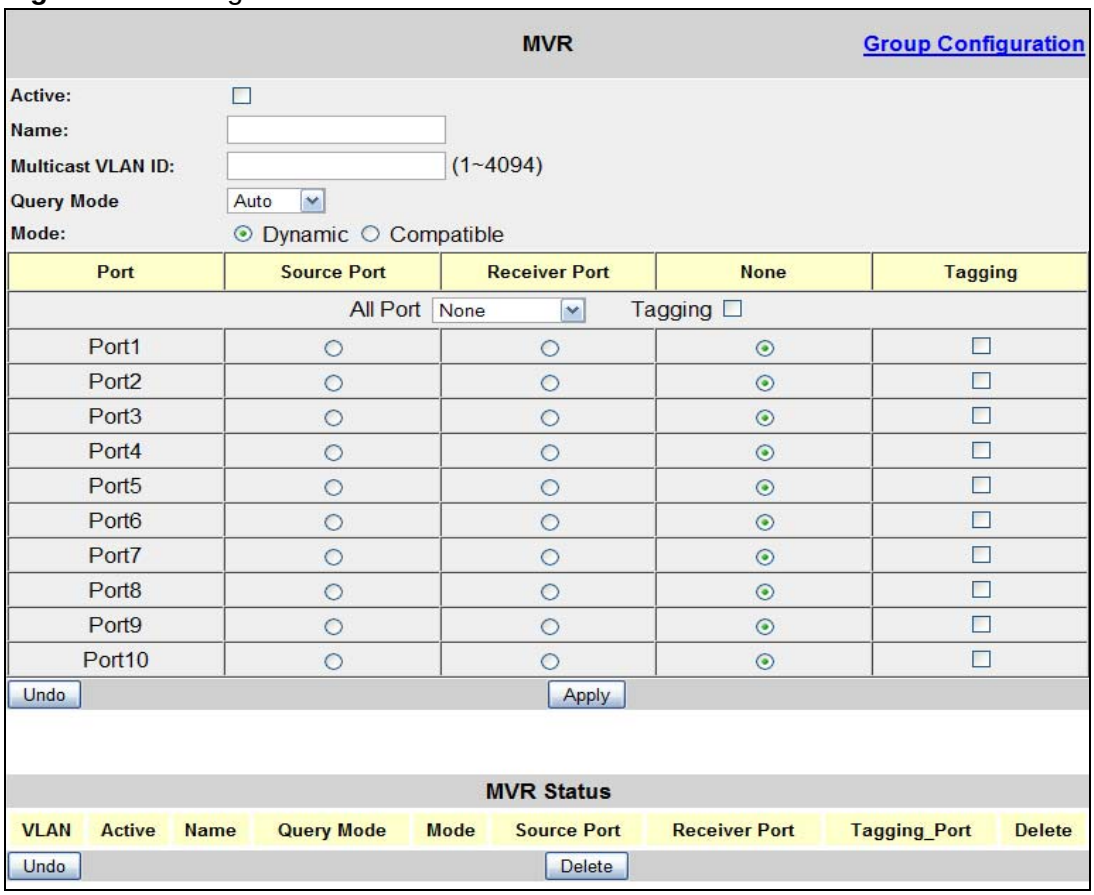
17.5 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Configuration > IGMP Menu** > **MVR** link to display the screen as shown next.

Note: You can create up to three multicast VLANs and up to 256 multicast rules on the MES-2110.

Note: Your MES-2110 automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 59 Configuration > IGMP Menu > MVR



The following table describes the related labels in this screen.

Table 49 Configuration > IGMP Menu > MVR

LABEL	DESCRIPTION
MVR	
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
Query Mode	Choose **Auto** to have the MES-2110 select the querier automatically, or **Disable** to turn this feature off.
Mode	Specify the MVR mode on the MES-2110. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the MES-2110 not to send IGMP reports.

Table 49 Configuration > IGMP Menu > MVR (continued)

LABEL	DESCRIPTION
Port	This field displays the port number on the MES-2110.
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
All Port	Use this to select between **Source Port**, **Receiver Port** or **None**.
Tagging	Select this checkbox if you want the ports to tag the VLAN ID in all outgoing frames transmitted.
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save Settings** link in the navigation panel to save your changes to the non-volatile memory when you are done configuring.
MVR Status	
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Query Mode	This field displays whether the query mode is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
Tagging Port	This field displays which port tags outgoing frames with the VLAN ID.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Undo	Click this to clear the **Delete** check boxes.

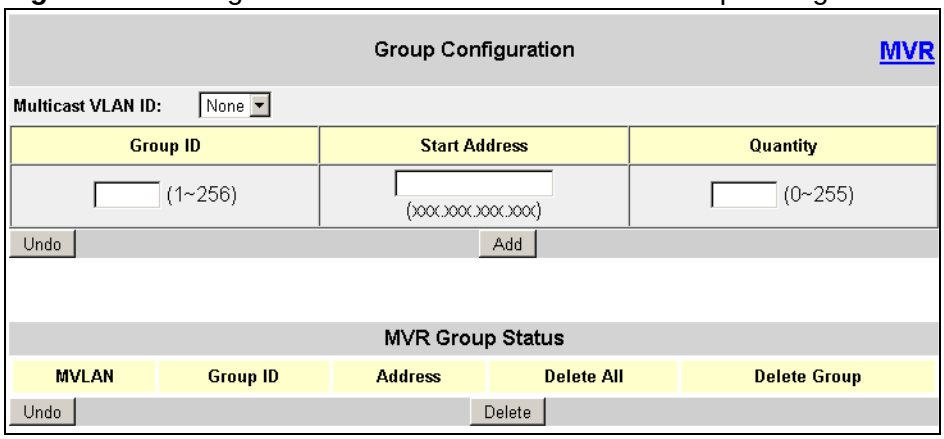
17.6 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.

Note: A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 60 Configuration > IGMP Menu > MVR > Group Configuration



The following table describes the labels in this screen.

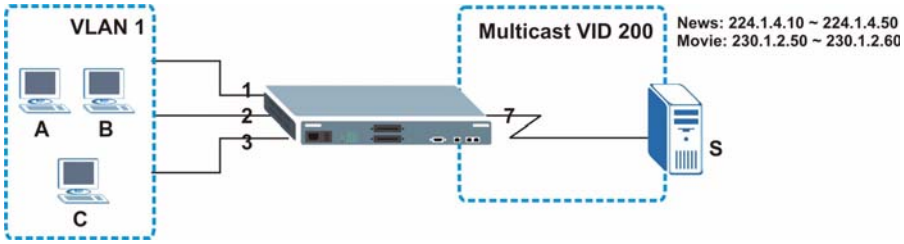
Table 50 Configuration > IGMP Menu > MVR > Group Configuration

LABEL	DESCRIPTION
Group Configuration	
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Group ID	Enter a group number for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 17.1.1 on page 123 for more information on IP multicast addresses.
Quantity	Specify the number of IP addresses to include in the multicast group.
Undo	Click this to load your last saved settings.
Add	Click **Add** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
MVR Group Status	
MVLAN	This field displays the multicast VLAN ID.
Group ID	This field displays the ID number that identifies the multicast group.
Address	This field displays the starting IP address of the multicast group.
Delet All	Select the check box and click the **Delete** button to remove all configured rules.
Delete Group	Select the check box in the **Delete Group** field and click **Delete** to remove the selected entry(ies) from the table.
Undo	Select this to clear the checkbox(es) in the table.

17.6.1 MVR Configuration Example

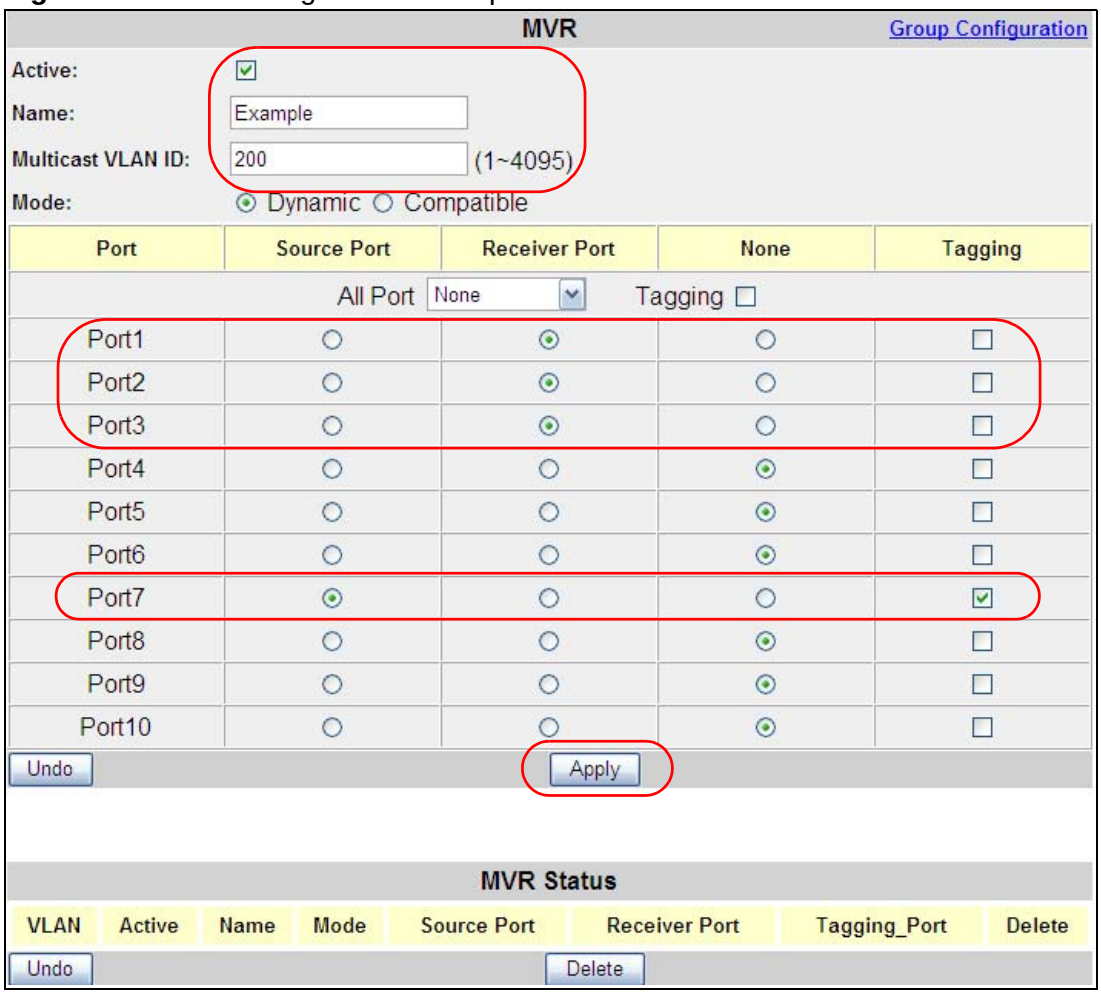
The following figure shows a network example where ports 1, 2 and 3 on the MES-2110 belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN are able to receive the traffic.

Figure 61 MVR Configuration Example



To configure the MVR settings on the MES-2110, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 62 MVR Configuration Example



To set the MES-2110 to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The

following figure shows an example where two multicast groups (Group ID **1** for **News** and Group ID **2** for **Movie**) are configured for the multicast VLAN 200.

Figure 63 MVR Group Configuration Example

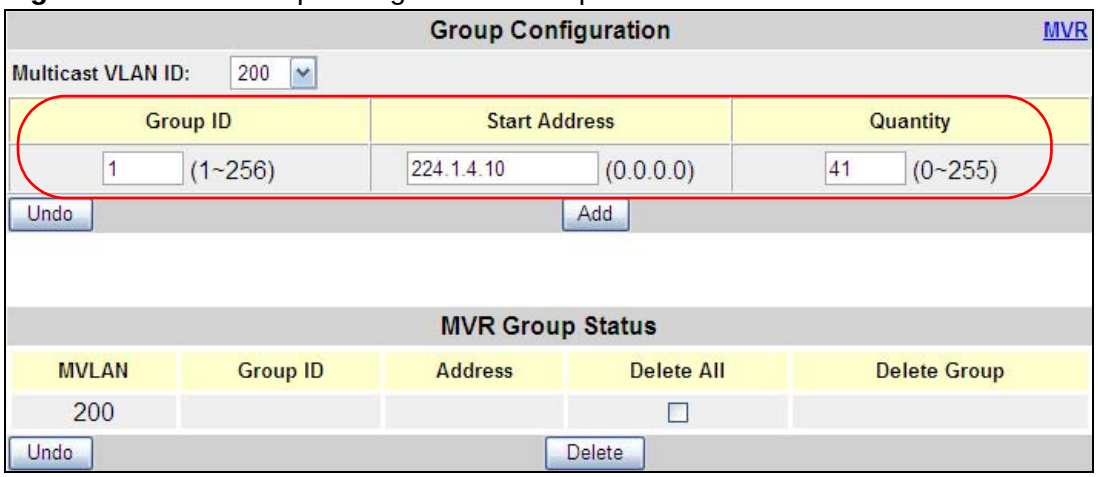
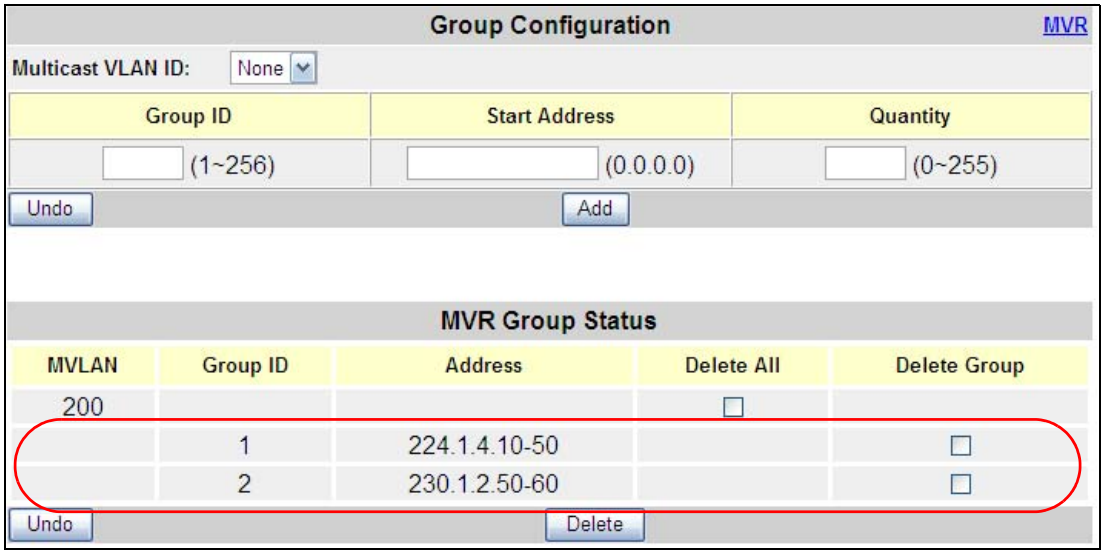


Figure 64 MVR Group Configuration Example



18

DHCP Relay Configuration

18.1 Overview

Configure DHCP relay on the MES-2110 if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the MES-2110 helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the MES-2110.

The MES-2110 can be configured as a global DHCP relay. This means that the MES-2110 forwards all DHCP requests from all domains to the same DHCP server. You can also configure the MES-2110 to relay DHCP information based on the VLAN membership of the DHCP clients.

18.1.1 DHCP Relay Agent Information

The MES-2110 can add information about the source of client DHCP requests that it relays to a DHCP server by adding Relay Agent information. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP Relay Agent feature adds an additional parameter to the Option 82 field. The Option 82 field is in the DHCP headers of client DHCP request frames that the MES-2110 relays to a DHCP server.

The following describes the DHCP relay information that the MES-2110 sends to the DHCP server:

Table 51 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone non-card based switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.

Table 51 Relay Agent Information

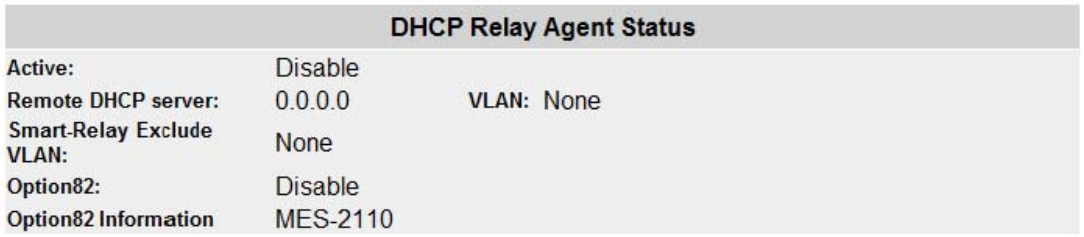
FIELD LABELS	DESCRIPTION
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Remote ID	(up to 64 bytes) This optional field is set on the **DHCP Relay Configuration** (Section 19.2 on page 143) screen

18.2 DHCP Relay Configuration

This screen allows you to configure the DHCP Relay Agent, which sends messages between DHCP clients and DHCP servers on different IP networks.

Click **Configuration > DHCP Relay Configuration** to open this screen.

Figure 65 Configuration > DHCP Relay Configuration



The following table describes the labels in this screen.

Table 52 Configuration > DHCP Relay Configuration

LABEL	DESCRIPTION
DHCP Relay Agent Configuration	
Active	Select this check box to enable DHCP relay.
Remote DHCP Server	Enter the IP address of a DHCP server in dotted decimal notation.
Smart Relay Exclude VLAN	Enter the VLAN ID to exclude from the DHCP relay function.
Option82	Select this to have the MES-2110 add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.

Table 52 Configuration > DHCP Relay Configuration (continued)

LABEL	DESCRIPTION
Option82 Information	Enter a unique identifier (such as the MES-2110's MAC address) for the DHCP relay agent. This must be globally unique. You can enter up to 64 ASCII characters.
Undo	Click this to reset the values in this screen to their last-saved values.
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
DHCP Relay Agent Status	
Active	This indicates whether DHCP relay is enabled or disabled.
Remote DHCP server	This indicates the remote DHCP server's IP address.
Smart-Relay Exclude VLAN	This indicates which VLAN IDs are excluded from the DHCP relay function.
Option82	This indicates whether Option82 is enabled or disabled.
Option82 Information	This indicates the remote ID of the DHCP relay agent.

19

IP Source Guard

19.1 Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP frames in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the MES-2110 receives a DHCP or ARP frame, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the MES-2110 forwards the frame. If there is not a binding, the MES-2110 discards the frame.

The MES-2110 builds the binding table by snooping DHCP frames (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP frames on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP frames on the network.

If you want to use dynamic bindings to filter unauthorized ARP frames (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

19.1.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP frames on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

19.1.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP frames that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The MES-2110 discards DHCP frames from trusted ports only if the rate at which DHCP frames arrive is too high. The MES-2110 learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The MES-2110 discards DHCP frames from untrusted ports in the following situations:

- The frame is a DHCP server frame (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the frame do not match any of the current bindings.
- The frame is a RELEASE or DECLINE frame, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP frames arrive is too high.

19.1.1.2 DHCP Snooping Static Binding Table

The MES-2110 stores the binding table in volatile memory. If the MES-2110 restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

19.1.1.3 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the MES-2110.

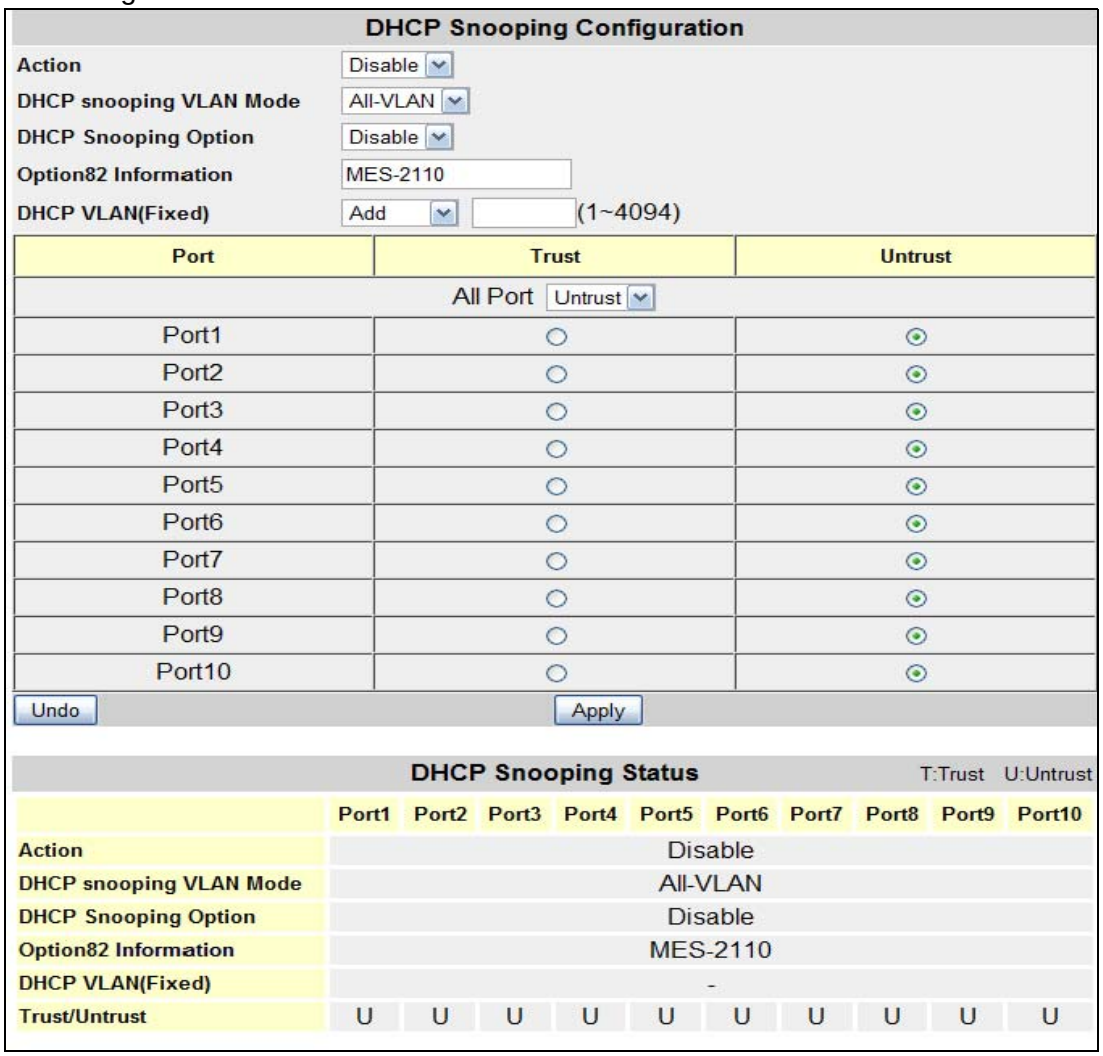
1. Enable DHCP snooping on the MES-2110.
2. Configure trusted and untrusted ports, and specify the maximum number of DHCP frames that each port can receive per second.

3 Configure static bindings.

19.2 DHCP Snooping Configuration

Use this screen to enable DHCP snooping on the MES-2110 and specify whether ports are trusted or untrusted ports for DHCP snooping. To open this screen, click **Configuration > IP Source Guard > DHCP > DHCP Snooping Configuration**.

Figure 66 Configuration > IP Source Guard > DHCP > DHCP Snooping Configuration



The following table describes the labels in this screen.

Table 53 Configuration > IP Source Guard > DHCP > DHCP Snooping Configuration

LABEL	DESCRIPTION
DHCP Snooping Configuration	
Action	Select **Enable** to have the MES-2110 use DHCP snooping . You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Select **Disable** if you do not want to use this feature. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
DHCP snooping VLAN Mode	Select **All-VLAN** to have the Switch forward DHCP frames of any VLANs to DHCP servers automatically. Select **Fixed** to have the Switch forward DHCP frames of a specific VLAN to DHCP servers.
DHCP Snooping Option	Select **Enable** to have the MES-2110 add DHCP relay agent option 82 information to DHCP requests that the MES-2110 relays to a DHCP server for each VLAN. Otherwise, select **Disable**.
Option82 Information	Enter a unique identifier (such as the MES-2110's MAC address) for the DHCP relay agent. This must be globally unique. You can enter up to 64 ASCII characters.
DHCP VLAN (Fixed)	Enter the ID of a static VLAN; the valid range is between 1 and 4094.
Port	This field displays the port number. If you configure the ***** port, the settings are applied to all of the ports.
Trust	Use this to set trusted ports. Trusted ports are connected to DHCP servers or other switches, and the MES-2110 discards DHCP frames from trusted ports only if the rate at which DHCP frames arrive is too high.
Untrust	Use this to set un-trusted ports. Untrusted ports are connected to subscribers, and the MES-2110 discards DHCP frames from untrusted ports in the following situations: • The frame is a DHCP server frame (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the frame do not match any of the current bindings. • The frame is a RELEASE or DECLINE frame, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP frames arrive is too high.
All Port	Use this to configure all ports as trusted or un-trusted ports.
Undo	Click this to reset the values in this screen to their last-saved values.

Table 53 Configuration > IP Source Guard > DHCP > DHCP Snooping Configuration (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the MES-2110's run-time memory. The MES-2110 loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
DHCP Snooping Status	
Action	This shows whether DHCP snooping is enabled or disabled.
DHCP snooping VLAN Mode	This shows whether the MES-2110 forwards DHCP frames of any VLANs or specific VLANs to DHCP servers.
DHCP Snooping Option	This specifies whether or not the MES-2110 enabled or disabled adding DHCP relay agent option 82 information to DHCP requests that the MES-2110 relays to a DHCP server for each VLAN.
Option82 Information	This indicates the remote ID of the DHCP relay agent.
DHCP VLAN (Fixed)	This shows the specific VLAN ID.
Trust/Untrust	This shows whether the port is trusted or un-trusted.

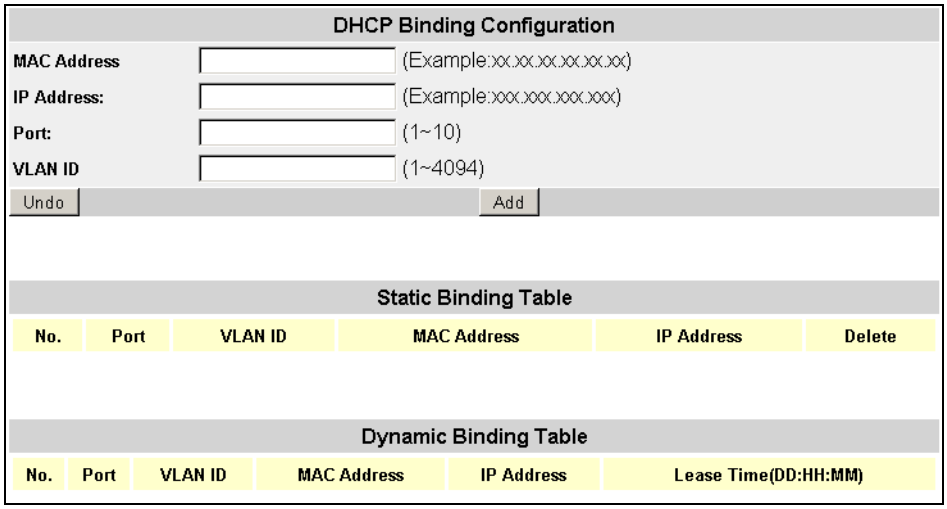
19.3 DHCP Binding Table

Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized frames in the network. The MES-2110 learns the bindings by snooping DHCP frames (dynamic bindings) and from information provided manually by administrators (static bindings).

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the

new static binding replaces the original one. Click **Configuration** > **DHCP Snooping** > **DHCP Binding Table** to open the following screen.

Figure 67 Configuration > DHCP Snooping > DHCP Binding Table



The following table describes the labels in this screen.

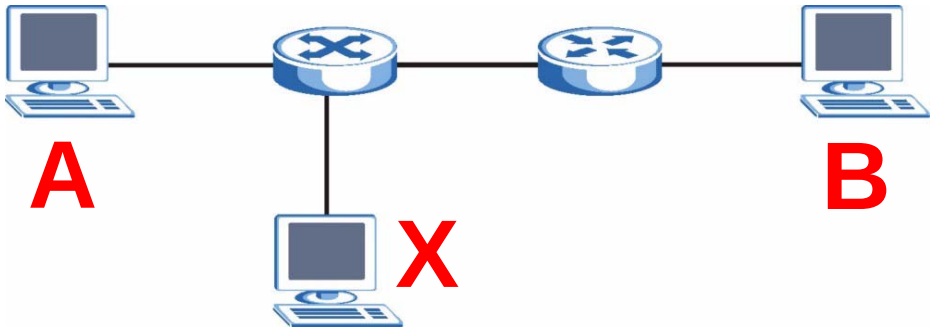
Table 54 Configuration > DHCP Snooping > DHCP Binding Table

LABEL	DESCRIPTION
DHCP Binding Configuration	
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
Port	Specify the port in the binding.
VLAN ID	Specify a VLAN ID if you want the MES-2110 to forward DHCP frames to DHCP servers on a specific VLAN. Leave the field blank if you do not want the MES-2110 to forward DHCP frames to a specific VLAN.
Undo	Click this to restore your last saved settings
Add	Click this to add the rule to the MES-2110.
Static/Dynamic Binding Table	
No.	This field displays a sequential number for each binding.
Port	This field displays the port number in the binding.
VLAN ID	This field displays the source VLAN ID in the binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Delete	Click this to delete a static binding rule.
Lease Time (DD:HH:MM)	This field displays how many days, hours and minutes the binding is valid; for example, **02:03:04** means the binding is still valid for 2 days, 3 hours and 4 minutes.

19.4 The ARP Inspection Screen

Use ARP inspection to filter unauthorized ARP frames on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 68 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

19.4.1 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the MES-2110.

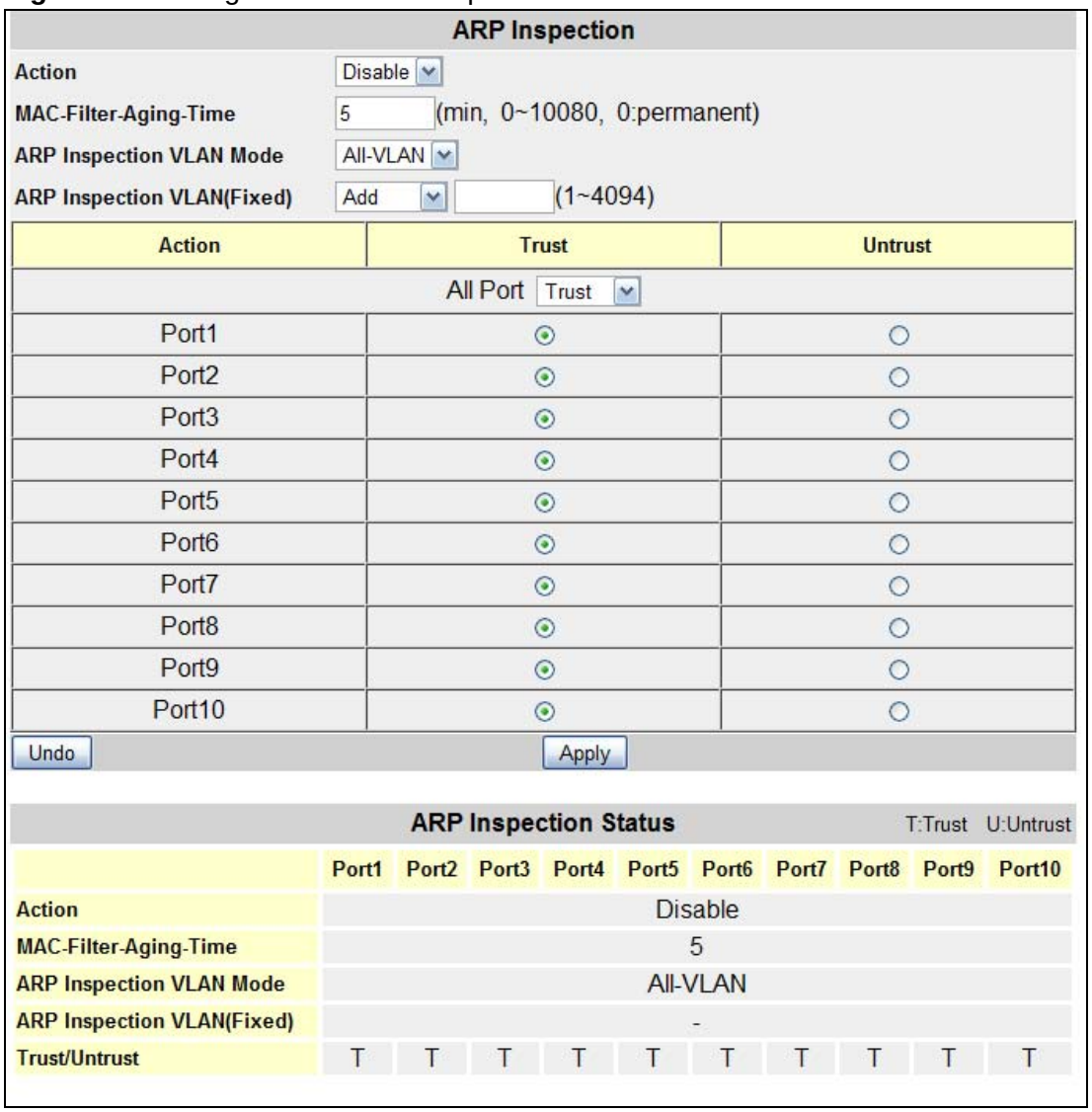
1 Configure DHCP snooping. See Section 19.1.1.3 on page 142.

Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the MES-2110 has enough time to build the binding table.

2 Enable ARP inspection on the MES-2110. See Section 19.4 on page 147 for more details about turning on this feature.

Click **IP Source Guard > ARP Inspection > ARP Inspection Config** to open the following screen.

Figure 69 Configuration > ARP Inspection



The following table describes the labels in this screen.

Table 55 Configuration > ARP Inspection

LABEL	DESCRIPTION
ARP Inspection	
Action	Use this to enable or disable the ARP inspection feature.
MAC-Filter-Aging-Time	Enter the number of minutes from 1-10080 that the MES-2110 retains MAC addresses in its MAC address table. Enter 0 to retain addresses permanently.

Table 55 Configuration > ARP Inspection

LABEL	DESCRIPTION
ARP Inspection VLAN Mode	Select **All-VLAN** to have the Switch look at all the VLANs on which ARP inspection is enabled. Select **Fixed** to have the Switch look at the specific VLANs on which ARP inspection in enabled..
ARP Inspection VLAN (Fixed)	Enter the ID of a static VLAN; the valid range is between 1 and 4094.
Action	This is the port number.
Trust	Use this to set trust ports.
Untrust	Use this to set un-trusted ports.
All Port	Use this to configure all ports as trusted or un-trusted ports.
ARP Inspection Status	
Action	This shows whether the ARP inspection feature is enabled or disabled on the MES-2110.
MAC-Filter-Aging-Time	This shows the number of minutes that the MES-2110 retains MAC addresses in its MAC address table.
ARP Inspection VLAN Mode	This shows whether the MES-2110 look at all VLANs or specific VLANs on which ARP inspection in enabled.
ARP Inspection VLAN (Fixed)	This shows the specific VLAN ID.
Trust/Untrust	This shows whether the port is trusted or un-trusted.

20 MAC

20.1 Overview

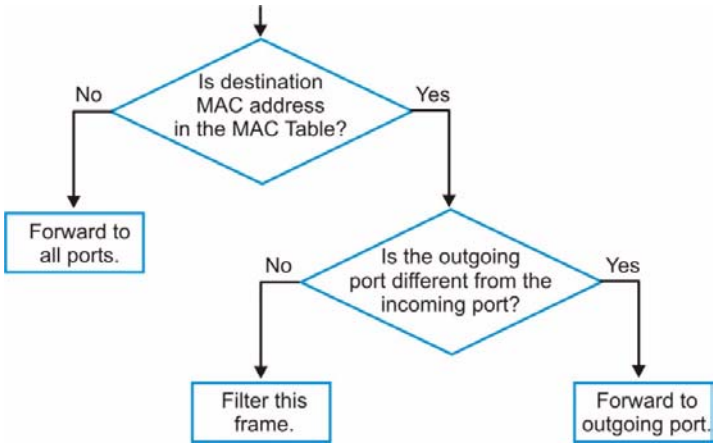
The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the MES-2110's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the MES-2110) or static (manually entered in the **Static MAC Forwarding** screen).

The MES-2110 uses the MAC table to determine how to forward frames. See the following figure.

1. The MES-2110 examines a received frame and learns the port on which this source MAC address came.
2. The MES-2110 checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
   - If the MES-2110 has already learned the port for this MAC address, then it forwards the frame to that port.
   - If the MES-2110 has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.

- If the MES-2110 has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

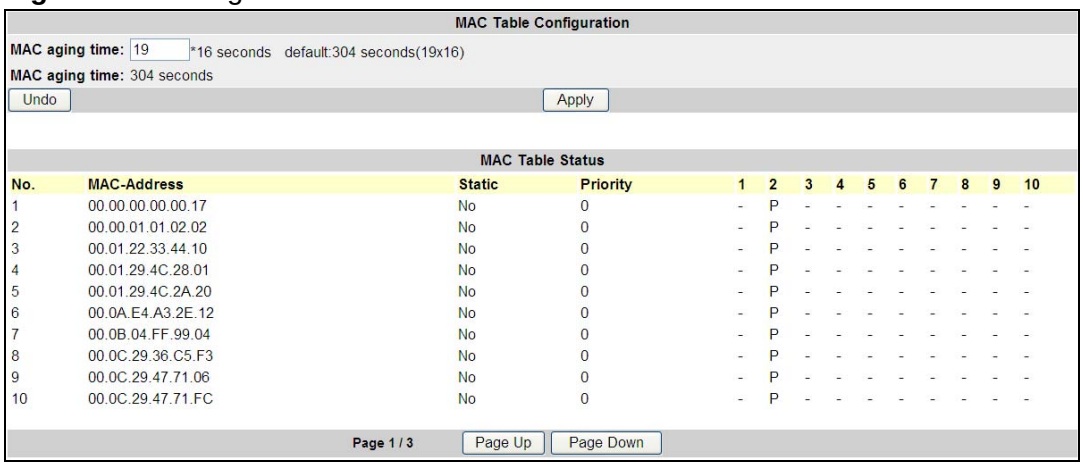
Figure 70 MAC Table Flowchart



20.2 The MAC Table Status Screen

Use this screen to configure the MAC aging time and view the MAC table. Click **Configuration** > **MAC Menu** > **MAC Table Status** to open the following screen.

Figure 71 Configuration > MAC Menu > MAC Table Status


MAC Table Configuration
MAC aging time: 19 *16 seconds default:304 seconds(19x16)
MAC aging time: 304 seconds
Undo
Apply
MAC Table Status
No. MAC-Address Static Priority 1 2 3 4 5 6 7 8 9 10
1 00.00.00.00.00.17 No 0 - P - - - - - - - -
2 00.00.01.01.02.02 No 0 - P - - - - - - - -
3 00.01.22.33.44.10 No 0 - P - - - - - - - -
4 00.01.29.4C.28.01 No 0 - P - - - - - - - -
5 00.01.29.4C.2A.20 No 0 - P - - - - - - - -
6 00.0A.E4.A3.2E.12 No 0 - P - - - - - - - -
7 00.0B.04.FF.99.04 No 0 - P - - - - - - - -
8 00.0C.29.36.C5.F3 No 0 - P - - - - - - - -
9 00.0C.29.47.71.06 No 0 - P - - - - - - - -
10 00.0C.29.47.71.FC No 0 - P - - - - - - - -
Page 1 / 3
Page Up
Page Down

The following table describes the labels in this screen.

Table 56 Configuration > MAC Menu > MAC Table Status

LABEL	DESCRIPTION
MAC Table Configuration	
MAC aging time	Enter a time from 16 to 4080 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
MAC aging time	This is the current MAC aging time.

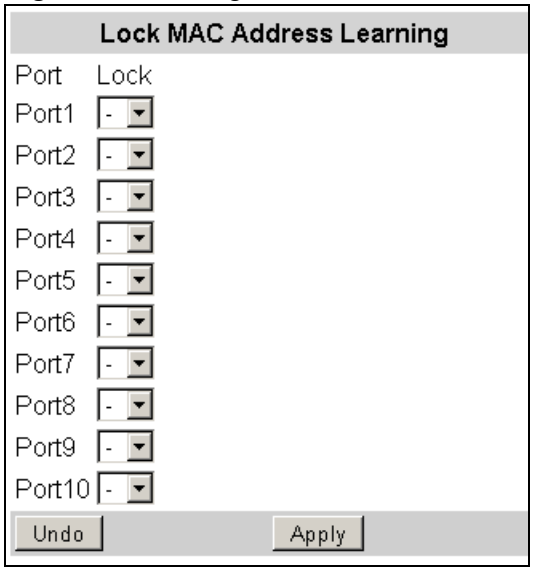
Table 56 Configuration > MAC Menu > MAC Table Status

LABEL	DESCRIPTION
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.
MAC Table Status	
No.	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
Static	This shows whether the MAC address is dynamic (learned by the MES-2110) or static (manually configured).
Priority	This shows the priority level of the MAC address
1-10	This shows the port from which the MAC address was learned.
Page Up/Down	Click this to view the previous or next page.

20.3 The Lock MAC Address Learning Screen

Use this screen to configure the MAC address learning settings. Click **Configuration** > **MAC Menu** > **Lock Learning MAC** to open the following screen.

Figure 72 Configuration > MAC Menu > Lock Learning MAC



The following table describes the labels in this screen.

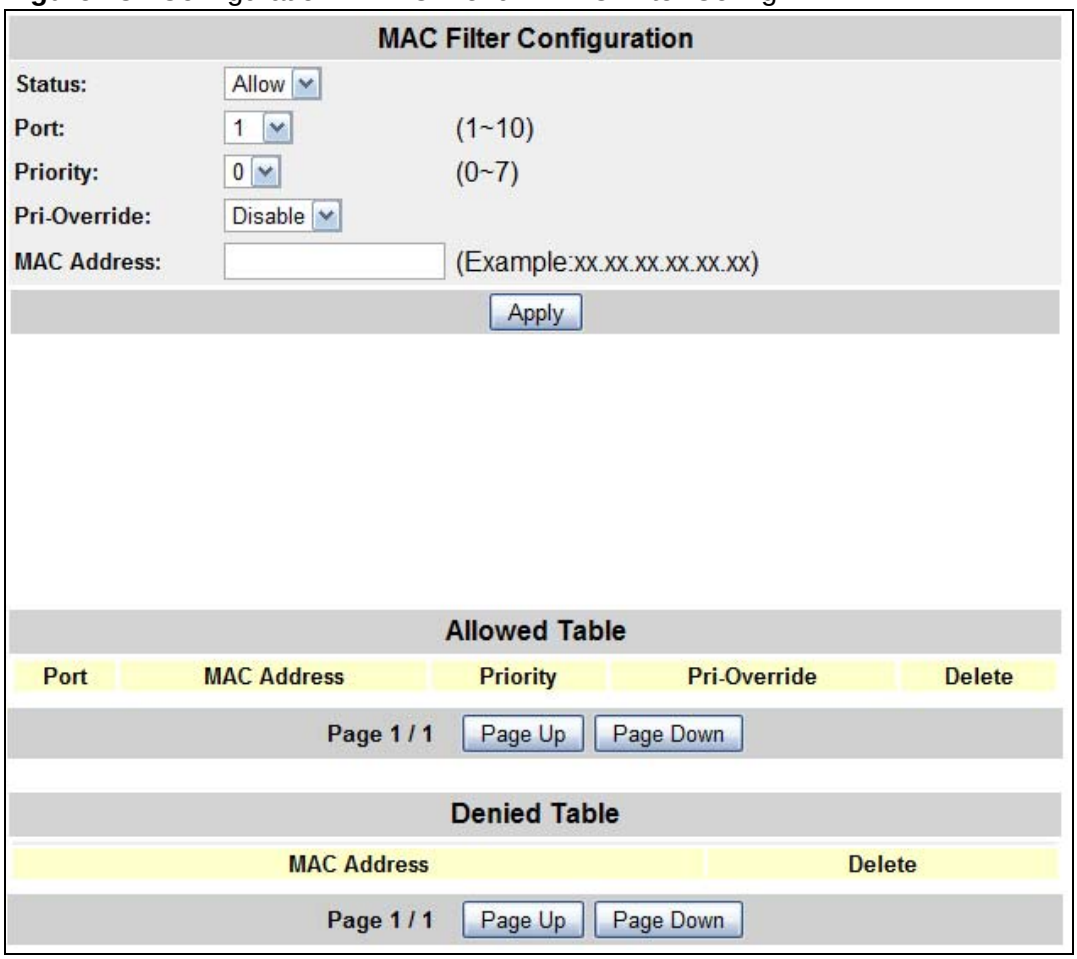
Table 57 Configuration > MAC Menu > Lock Learning MAC

LABEL	DESCRIPTION
Port	This is the port number.
Lock	MAC address learning reduces outgoing broadcast traffic. Use this to activate MAC address learning on the port.
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

20.4 The MAC Filter Configuration Screen

Use this screen to configure and view the MAC filter settings. Click **Configuration** > **MAC Menu** > **MAC Filter Config** to open the following screen.

Figure 73 Configuration > MAC Menu > MAC Filter Config



The following table describes the labels in this screen.

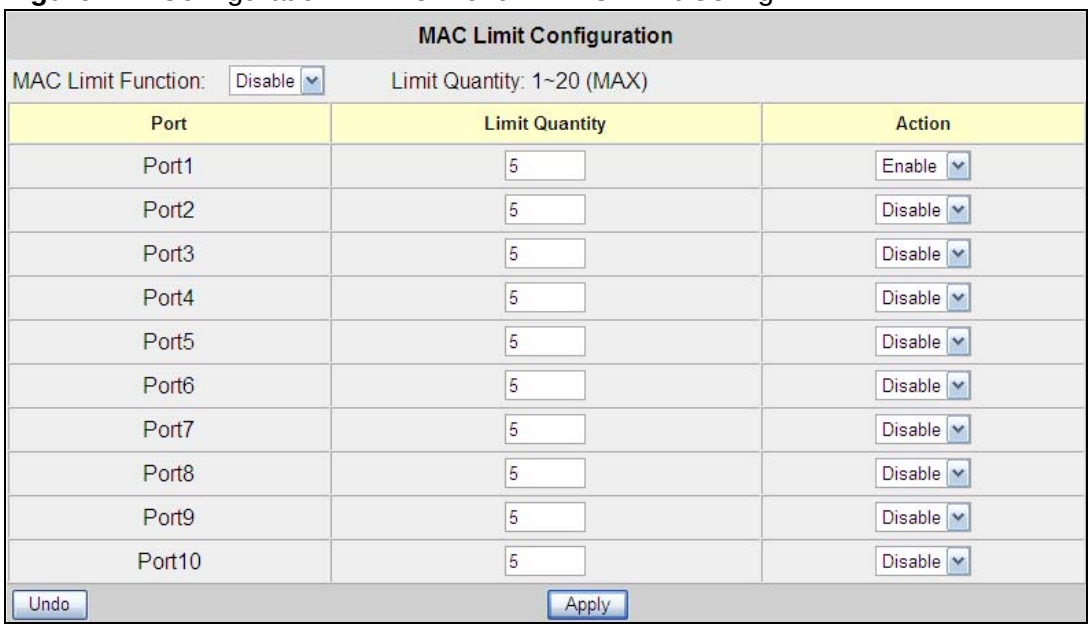
Table 58 Configuration > MAC Menu > MAC Filter Config

LABEL	DESCRIPTION
MAC Filter Configuration	
Status	Use this to determine whether to allow or deny traffic transmitted from the source MAC address.
Port	Select the port through which traffic from the source MAC address is transmitted.
Priority	Select a priority level from 0 to 7.
Pri-Override	Use this to ignore the priority level assigned to the transmitted frames.
MAC Address	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.
Allowed Table	
Port	This is the port number through which traffic from the source MAC address is transmitted.
MAC Address	This is the source MAC address.
Priority	This shows the priority level.
Pri-Override	This shows whether priority level override is enabled or disabled.
Delete	Click this to remove the rule.
Page Up/Down	Click this to view the previous or next page.
Denied Table	
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.
MAC Address	This is the source MAC address.
Delete	Click this to remove the rule.
Page Up/Down	Click this to view the previous or next page.

20.5 The MAC Limit Configuration Screen

Use this screen to limit the number of MAC addresses that can be learned on a port. Click **Configuration** > **MAC Menu** > **MAC Limit Config** to open the following screen.

Figure 74 Configuration > MAC Menu > MAC Limit Config



The following table describes the labels in this screen.

Table 59 Configuration > MAC Menu > MAC Limit Config

LABEL	DESCRIPTION
MAC Limit Function	Use this to enable or disable the MAC address limit feature.
Port	This is the port number.
Limit Quantity	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **MAC Table Status** screen.
Action	Enable the MAC limit function on this port. The MES-2110 forwards frames whose MAC address(es) is in the MAC address table on this port. frames with no matching MAC address(es) are dropped. Disable the MAC limit function to forwards all frames on this port.
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

21 QoS

21.1 Overview

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All frames in the flow are given the same priority. You can use QoS to give different priorities to different frame types to solve performance degradation when there is network congestion.

21.2 The QoS Base Configuration Screen

Queuing algorithms allow switches to maintain separate queues for frames from each individual source or flow and prevent a source from monopolizing the bandwidth.

All High Before Low Queuing

All high before low services queues based on priority only. As traffic comes into the MES-2110, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

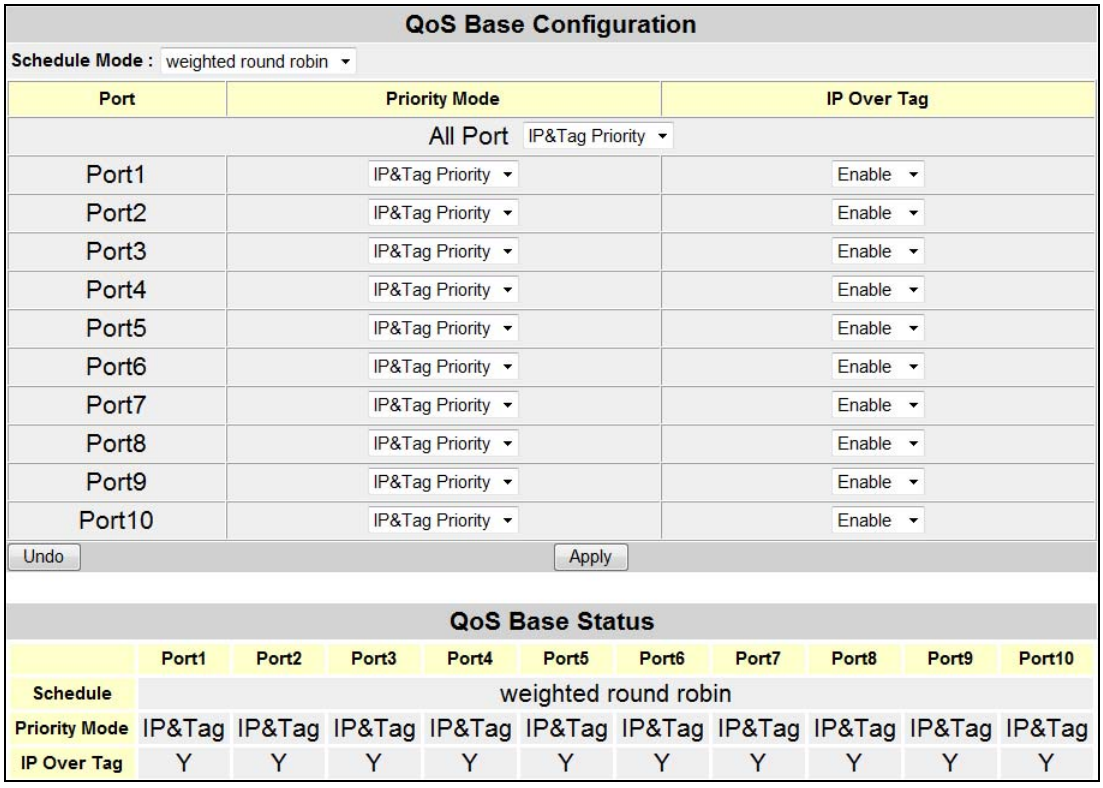
Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can

handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

21.2.1 Configuring the Base Configuration Screen

Use this screen to configure queuing settings on the MES-2110. Click **Configuration** > **QoS Menu** > **Base Configuration** to open the following screen.

Figure 75 Configuration > QoS Menu > Base Configuration


QoS Base Configuration
Schedule Mode : weighted round robin
Port
Priority Mode
IP Over Tag
All Port IP&Tag Priority
Port1 IP&Tag Priority Enable
Port2 IP&Tag Priority Enable
Port3 IP&Tag Priority Enable
Port4 IP&Tag Priority Enable
Port5 IP&Tag Priority Enable
Port6 IP&Tag Priority Enable
Port7 IP&Tag Priority Enable
Port8 IP&Tag Priority Enable
Port9 IP&Tag Priority Enable
Port10 IP&Tag Priority Enable
Undo
Apply
QoS Base Status
Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10
Schedule weighted round robin
Priority Mode IP&Tag IP&Tag IP&Tag IP&Tag IP&Tag IP&Tag IP&Tag IP&Tag IP&Tag IP&Tag
IP Over Tag Y Y Y Y Y Y Y Y Y Y

The following table describes the labels in this screen.

Table 60 Configuration > QoS Menu > Base Configuration

LABEL	DESCRIPTION
QoS Base Configuration	
Schedule Mode	Select **all high before low** or **weighted round robin**. All high before low queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight. Queues with larger weights get more service than queues with smaller weights.

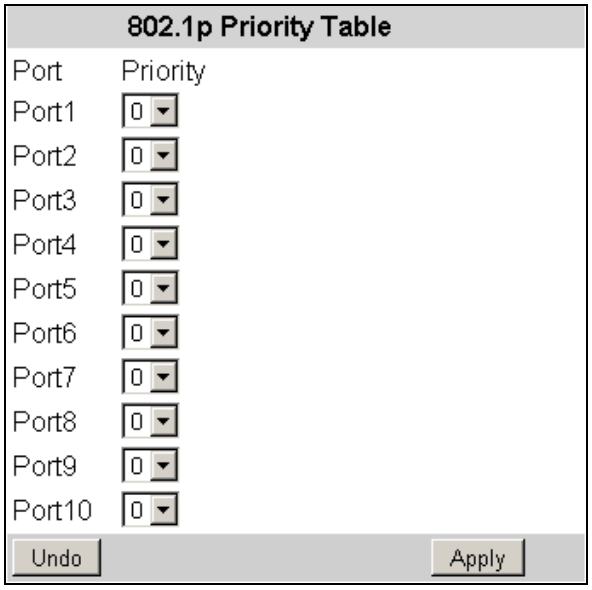
Table 60 Configuration > QoS Menu > Base Configuration

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Priority Mode	Select a priority mode for the port. **802.1p Priority** uses port priority as queuing basis. Assign a priority level to each port in the **802.1p Priority** screen (Section 21.3 on page 160). **Tag Priority** uses VLAN tag priority as queuing basis. See Section 21.4 on page 161 for more details on configuring tag priority. **IP ToS Priority** uses IP DSCP priority as queuing basis. See Section 21.5 on page 161 for more details on configuring IP DSCP priority. **IP & Tag Priority** uses both IP DSCP priority and tag priority as queuing basis.
IP Over Tag	Use this to enable or disable IP Over Tag on the port. When you enable this feature and the MES-2110 receives a frame containing both IP DSCP and tag priority information, the MES-2110 will only use the IP DSCP priority information.
All Port	Use this to set the priority mode for all ports.
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.
QoS Base Status	
Port1-10	This is the port number.
Schedule	This is the schedule mode used on the MES-2110.
Priority Mode	This is the priority mode used on the port.
IP Over Tag	This shows whether the IP over tag feature is enabled or disabled on the MES-2110.

21.3 The 802.1p Priority Table

Use this screen to assign a priority level for each port. Click **Configuration** > **QoS Menu** > **802.1p Priority** to open the following screen.

Figure 76 Configuration > QoS Menu > 802.1p Priority



The following table describes the labels in this screen.

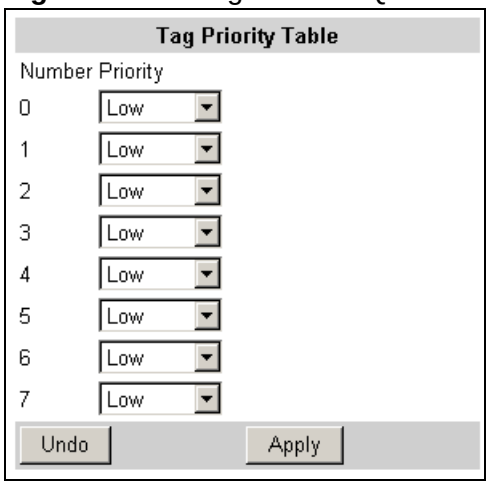
Table 61 Configuration > QoS Menu > 802.1p Priority

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Priority	Assign a priority level to the port.
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

21.4 The Tag Priority Table

Click **Configuration** > **QoS Menu** > **Tag Priority** to open the following screen.

Figure 77 Configuration > QoS Menu > Tag Priority



The following table describes the labels in this screen.

Table 62 Configuration > QoS Menu > Tag Priority

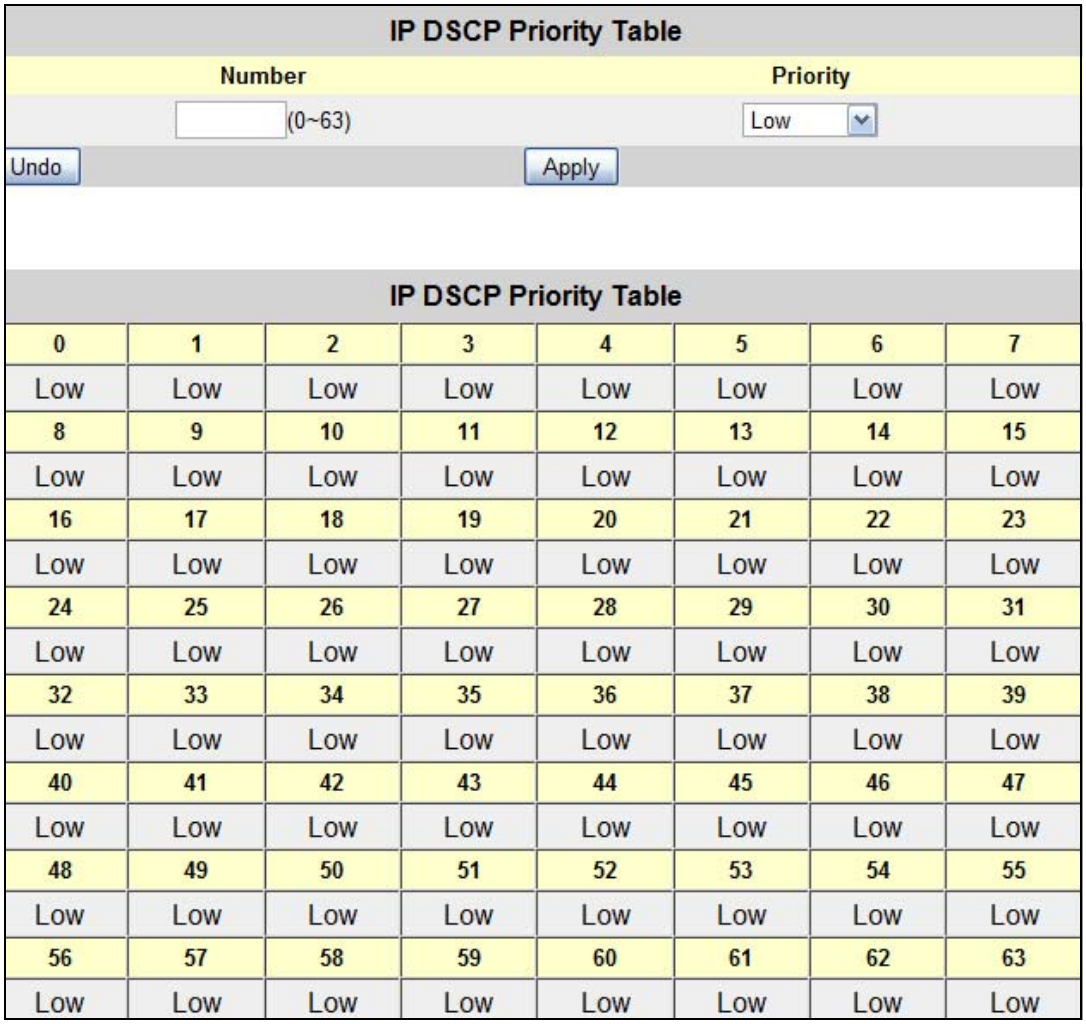
LABEL	DESCRIPTION
Number	This is the IEEE 802.1p priority level.
Priority	Use this to assign the tag priority level to one of the MES-2110's queue level (**Low**, **Normal**, **Preferred** or **High**).
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

21.5 The IP DSCP Priority Table

DiffServ is a class of service (CoS) model that marks frames so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Frames are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the frames differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

Use this to assign DSCP priority settings. Click **Configuration** > **QoS Menu** > **IP DSCP Priority** to open the following screen.

Figure 78 Configuration > QoS Menu > IP DSCP Priority



IP DSCP Priority Table

Number		Priority
	(0~63)	Low

Undo Apply

IP DSCP Priority Table

0	1	2	3	4	5	6	7
Low	Low	Low	Low	Low	Low	Low	Low
8	9	10	11	12	13	14	15
Low	Low	Low	Low	Low	Low	Low	Low
16	17	18	19	20	21	22	23
Low	Low	Low	Low	Low	Low	Low	Low
24	25	26	27	28	29	30	31
Low	Low	Low	Low	Low	Low	Low	Low
32	33	34	35	36	37	38	39
Low	Low	Low	Low	Low	Low	Low	Low
40	41	42	43	44	45	46	47
Low	Low	Low	Low	Low	Low	Low	Low
48	49	50	51	52	53	54	55
Low	Low	Low	Low	Low	Low	Low	Low
56	57	58	59	60	61	62	63
Low	Low	Low	Low	Low	Low	Low	Low

The following table describes the labels in this screen.

Table 63 Configuration > QoS Menu > IP DSCP Priority

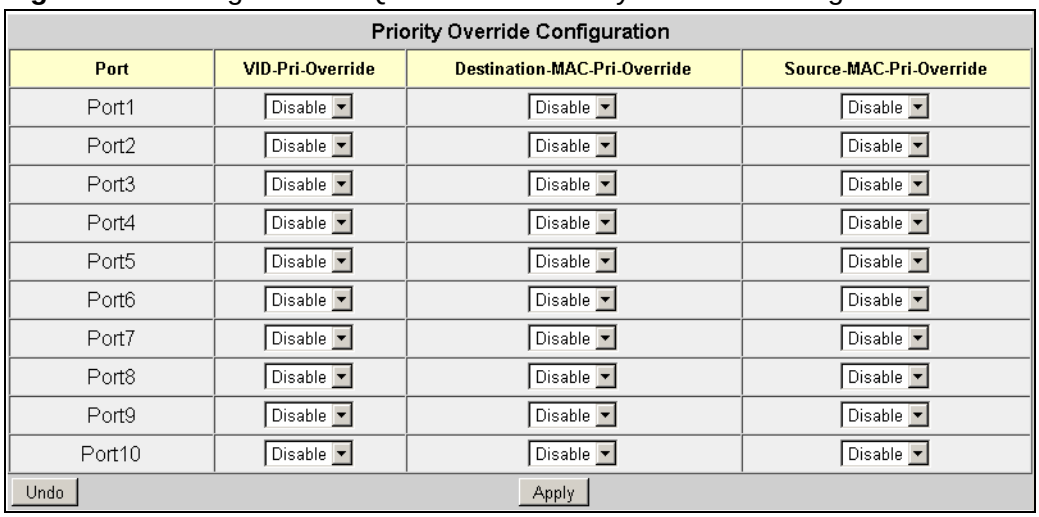
LABEL	DESCRIPTION
Number	Enter the DSCP classification identification number (0-63).
Priority	Assign a MES-2110's priority level (**Low**, **Normal**, **Preferred** or **High**) to the DSCP value.
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

21.6 The Priority Override Configuration Screen

Use this screen to apply the QoS settings of the MES-2110 to its DHCP clients. The MES-2110 ignores the priority levels assigned to the transmitted frames on the ports, source MAC addresses and destination MAC addresses.

Click **Configuration** > **QoS Menu** > **Priority Override Configuration** to open the following screen.

Figure 79 Configuration > QoS Menu > Priority Override Configuration



The following table describes the labels in this screen.

Table 64 Configuration > QoS Menu > Priority Override Configuration

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
VID-Pri-Override	Select **Enable** to have the MES-2110 ignore the priority level assigned to the transmitted frames on this port. Select **Disable** if you do not want to use this feature. This is selected by default.
Destination-MAC-Pri-Override	Select **Enable** to have the MES-2110 ignore the priority level assigned to the transmitted frames on the destination MAC address. Select **Disable** if you do not want to use this feature. This is selected by default.
Source-MAC-Pri-Override	Select **Enable** to have the MES-2110 ignore the priority level assigned to the transmitted frames on the source MAC address. Select **Disable** if you do not want to use this feature. This is selected by default.

Table 64 Configuration > QoS Menu > Priority Override Configuration

LABEL	DESCRIPTION
Undo	Click this to load your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

22

Mgmt Config and System Restart Menu

22.1 Overview

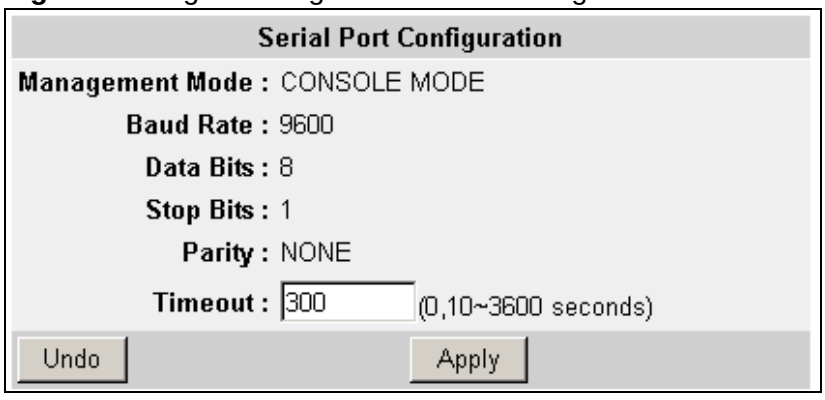
This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

22.2 The Serial Port Configuration Screen

Use this screen to view the parameters for local management. Configure a computer's terminal emulation software with the displayed parameters to manage the MES-2110. Connect the male 9-pin end of the console cable to the console port of the MES-2110. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

Click **Mgmt Config** > **Serial Port Config** to open the following screen.

Figure 80 Mgmt Config > Serial Port Config

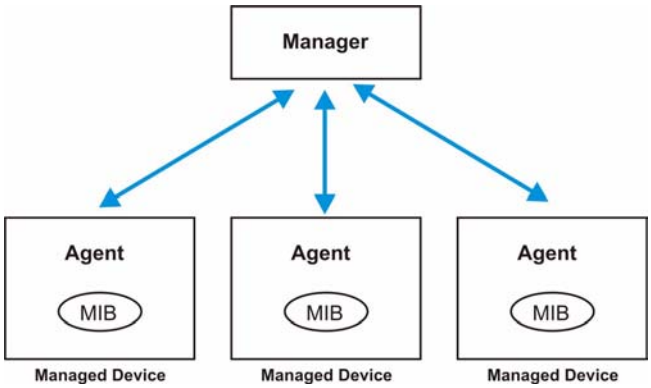


Specify the amount of time (in seconds) before the console session disconnects automatically. If you set the timeout to 0 second, the console session never expires. Click **Apply** to save your changes.

22.3 The SNMP Configuration Screens

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the MES-2110 through the network via SNMP version one (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 81 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the MES-2110). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 65 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

22.3.1 The SNMP Communities Screen

Use this screen to configure the SNMP communities. Click **Mgmt Config** > **SNMP Config** > **SNMP Communities** to open the following screen.

Figure 82 Mgmt Config > SNMP Config > SNMP Communities

The following table describes the labels in this screen.

Table 66 Mgmt Config > SNMP Config > SNMP Communities

LABEL	DESCRIPTION
GET	Enter the Get community string, which is the password for the incoming Get- and GetNext- requests from the management station.
SET	Enter the Set community string, which is the password for incoming Set- requests from the management station.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

22.3.2 The IP Trap Manager Screen

An IP trap manager receives authentication failure messages or other trap messages about the MES-2110's activities. The MES-2110 supports up to five trap

managers. Use this screen to configure the trap manager settings. Click **Mgmt Config** > **SNMP Config** > **IP Trap Manager** to open the following screen.

Figure 83 Mgmt Config > SNMP Config > IP Trap Manager

The following table describes the labels in this screen.

Table 67 Mgmt Config > SNMP Config > IP Trap Manager

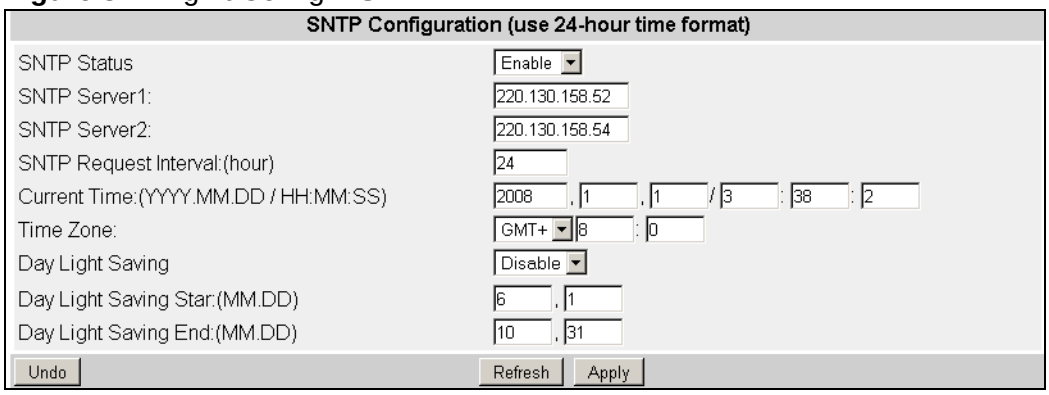
LABEL	DESCRIPTION
IP Address	Enter the IP addresses of up to five managers to send your SNMP traps to.
Community Name	Enter the community string.
Status	Use this to enable or disable the trap manager feature.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

22.4 The SNTP Screen

Use this screen to configure the time settings on the MES-2110. You can configure the MES-2110 to get the time and date information from a time server using Simple Network Time Protocol (SNTP). You can also configure two servers. If the first one is down, the MES-2110 will try to connect to the second one.

Click **Mgmt Config** > **SNTP** to open the following screen.

Figure 84 Mgmt Config > SNTP



The following table describes the labels in this screen.

Table 68 Mgmt Config > SNTP

LABEL	DESCRIPTION
SNTP Status	Use this to enable or disable time server for the MES-2110.
SNTP Server 1 and 2	Enter the IP address of your time server.
SNTP Request Interval	Specify how often (in hours) should the MES-2110 synchronize with the time server. For example, if you set the field to 2 hours, the MES-2110 synchronizes date/time with the time server every 2hours.
Current Time	Specify the date (in year, month and day format) and time (in hour, minute and second format).
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone.
Day Light Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Enable this option if you use Daylight Saving Time.
Day Light Saving Start	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. You'll have to manually configure the date every year as the date changes every year.

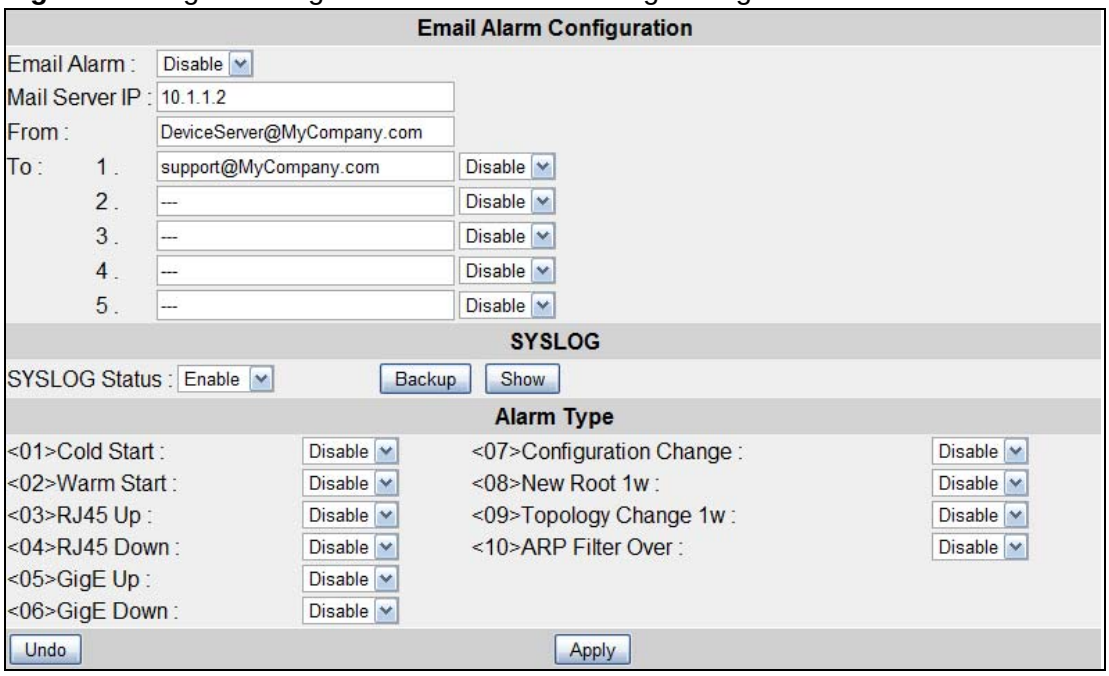
Table 68 Mgmt Config > SNTP

LABEL	DESCRIPTION
Day Light Saving End	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. You'll have to manually configure the date every year as the date changes every year.
Undo	Click this to restore your last saved settings.
Refresh	Click this to reset the data for the field(s).
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

22.5 Alarms and Logs

Use this screen to configure the mail server, the syslog and alarm settings. Click **Mgmt Config** > **Email Alarm & SYSLog Config** to open the following screen.

Figure 85 Mgmt Config > Email Alarm & SYSLog Config



The following table describes the labels in this screen.

Table 69 Mgmt Config > Email Alarm & SYSLog Config

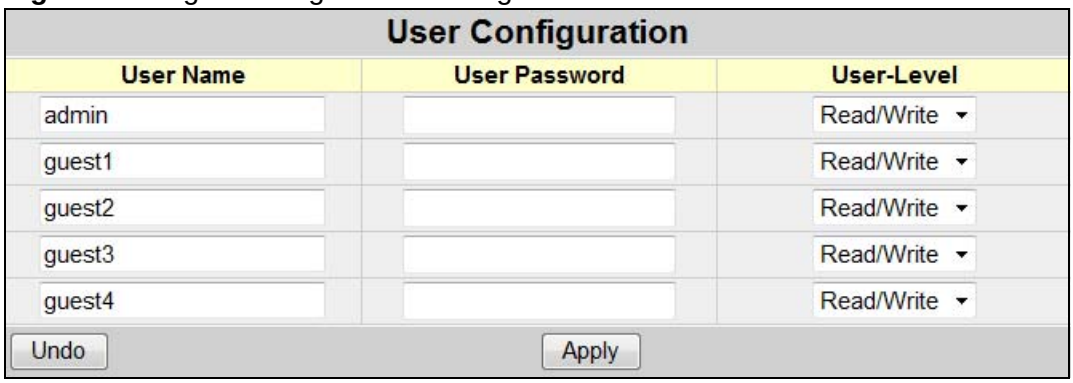
LABEL	DESCRIPTION
Email Alarm Configuration	
Email Alarm	Use this to enable or disable the e-mail alarm system.
Mail Server IP	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alerts messages will not be sent via e-mail.
From	Assign a valid e-mail address to the MES-2110.
To	The MES-2110 sends logs to the e-mail addresses specified in this field. If this field is left blank, the MES-2110 does not send logs via e-mail.
SYSLOG	
SYSLOG Status	Use this to enable or disable syslog logging.
Backup	Click this save syslog file to a TFTP server.
Show	Click this to show a complete list of syslog messages.
Alarm Type	Select the categories of alarm that you want to record and send an e-mail alarm.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

22.6 The User Configuration Screen

Use this screen to configure user names, passwords and access right for up to five user accounts. Click Mgmt Config > User Config to open the following screen.

Note: It is recommended that only one user log in and manage the device at a time. When multiple users configure the device settings simultaneously, changes may be overwritten.

Figure 86 Mgmt Config > User Config



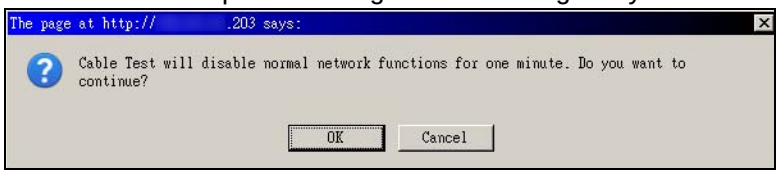
The following table describes the labels in this screen.

Table 70 Mgmt Config > User Config

LABEL	DESCRIPTION
User Name	Enter a name to identify the user account. You can type up to 15 characters using characters found on a standard keyboard.
User Password	Enter a password associated with the user name. You can type up to 15 characters using characters found on a standard keyboard.
User-Level	Assign access rights for the user account. **Read/Write** users can manage the MES-2110 settings as an administrator. **Read Only** users can only view the MES-2110 settings.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

22.7 The Cable Test Screen

Use this feature to diagnose the connection on each port. Click **Mgmt Config** > **Cable Test** to open a dialogue box asking for your confirmation.


The page at http:// .203 says:
Cable Test will disable normal network functions for one minute. Do you want to continue?
OK
Cancel

Click **OK** to start the test. The test results are shown as follows.

Figure 87 Mgmt Config > Host Denial-of-Service Protection

Cable Test

Port	PHY (RX/TX)	Test	Status	CableLength
1	Link-Down			
2	Link-Down			
3	Link-Down			
4	Link-Down			
5	Link-Down			
6	Link-Down			
7	Link-Down			
8	100 RX	pass	normal	
8	100 TX	pass	normal	
9	Link-Down			
10	Link-Down			

TEST

The following table describes the labels in this screen.

Table 71 Mgmt Config > Host Denial-of-Service Protection

LABEL	DESCRIPTION
Port	This is the port number.
PHY (RX/TX)	This shows if data is flowing through the ports on the MES-2110. If no data is passing through a port, this shows **Link-Down**. Otherwise, the number indicates the maximum size of packets during data transmission in the port.
Test	If the cable is well connected to the port, this shows **Pass**. Otherise, this shows **Fail**.
Status	If the cable is well connected to the port, this is **Normal**. If the connection is down, you see an **Open** status.

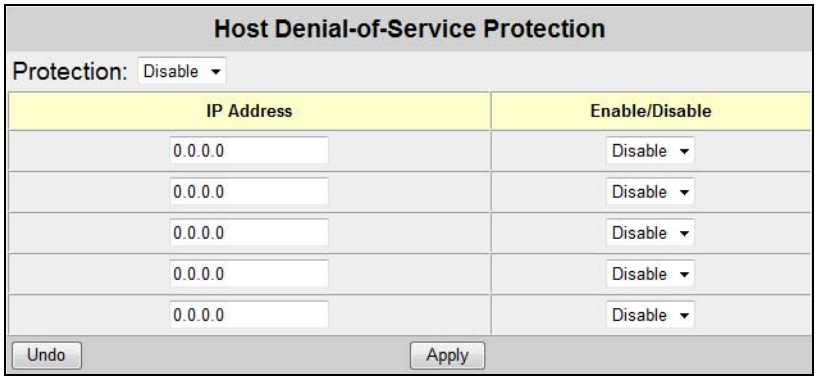
Table 71 Mgmt Config > Host Denial-of-Service Protection

LABEL	DESCRIPTION
CableLength	This shows the length of the cable connected to the port.
TEST	Click this to run the test again.

22.8 The Host DoS Protection

You can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the MES-2110. When you turn on this feature, only the trusted IP addresses listed in this screen can use remote management to access the MES-2110. Click **Mgmt Config** > **Host Denial-of-Service Protection** to open the following screen.

Figure 88 Mgmt Config > Host Denial-of-Service Protection



The following table describes the labels in this screen.

Table 72 Mgmt Config > Host Denial-of-Service Protection

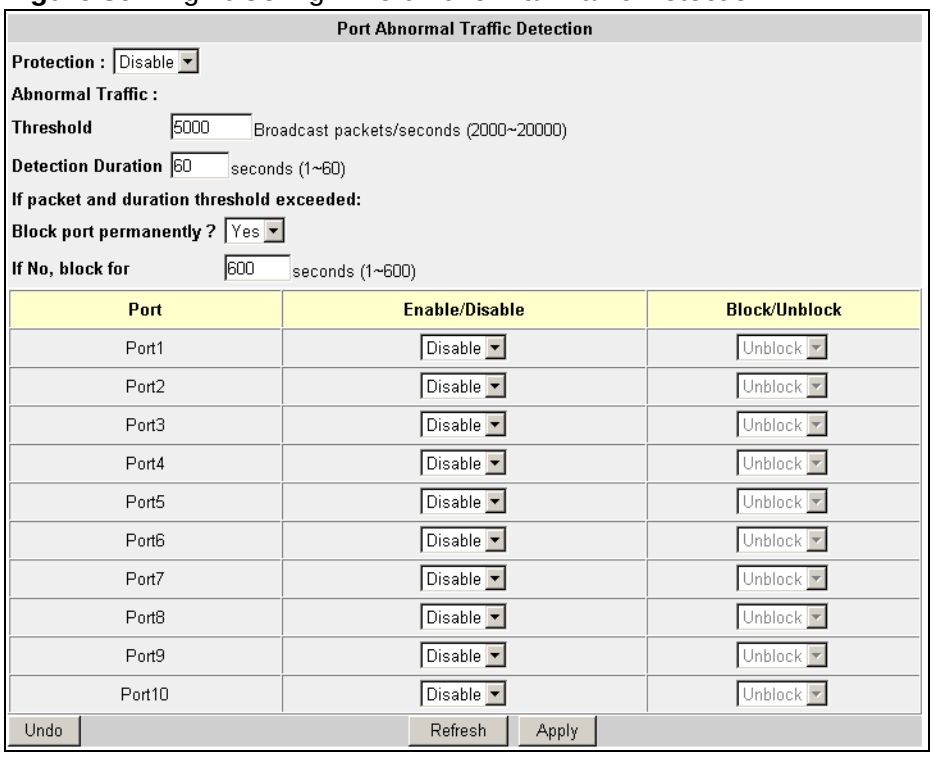
LABEL	DESCRIPTION
Protection	Use this to enable or disable host denial-of-service protection.
IP Address	Configure the IP address of the trusted computer from which you can manage this MES-2110. The MES-2110 checks if the client IP address of a computer requesting a service or protocol matches the range set here. The MES-2110 immediately disconnects the session if it does not match.
Enable/Disable	Select **Enable** to activate this secured client set. Select **Disable** if you wish to temporarily disable the set without deleting it.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device’s run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

22.9 The Port Abnormal Traffic Detection Screen

This MES-2110 can detect excessive broadcasts or transmission load on a port and temporarily or permanently block traffic transmission on each port. Use this screen to configure the MES-2110's threshold settings for blocking a port. You can also have the Switch unblock a port when it is no longer receiving large broadcast packets.

Click **Mgmt Config** > **Port Abnormal Traffic Detection** to open the following screen.

Figure 89 Mgmt Config > Port Abnormal Traffic Detection



The following table describes the labels in this screen.

Table 73 Mgmt Config > Port Abnormal Traffic Detection

LABEL	DESCRIPTION
Protection	Use this to enable or disable abnormal traffic detection on the MES-2110.
Abnormal Traffic	Set the rules for abnormal traffic in the fields described below.
Threshold	Specify a threshold value (in broadcast packets per second). If transmission load on a port exceeds this threshold, the MES-2110 blocks the port. The block can be blocked permanently or for a period of time, depending on what you specify in this screen (see fields below).

Table 73 Mgmt Config > Port Abnormal Traffic Detection

LABEL	DESCRIPTION
Detection Duration	Specify for how long (up to 60 seconds) the threshold is exceeded before the MES-2110 blocks the port. This allows the port(s) to exceed the threshold for a short time period depending on the number of seconds you specify. The port is blocked when the transmission load continues and the number of seconds has expired.
If packet and duration threshold exceeded	
Block port permanently	Select **Yes** to block the port for good if traffic exceeds the threshold for a certain time. You can manually unblock a port in the **Block/Unblock** field. However the port is only unblocked when it is not receiving excessive traffic anymore.
If No, block for N seconds	Specify for how long the MES-2110 will block the port if traffic exceeds the threshold.
Port	This shows the port number(s) that you can configure.
Enable/Disable	If you enabled abnormal traffic detection on the MES-2110, use this to enable or disable abnormal traffic detection on a specific port. The rules you set will only apply to ports that are set to **Enable**.
Block/Unblock	Use this field to manually block or unblock a port. Select **Block** to have the Switch block a port according to the abnormal traffic detection values you specified in this screen. Select **Unblock** to have the Switch unblock a previously blocked port when it is not receiving abnormal traffic anymore.
Undo	Click this to restore your last saved settings.
Apply	Click **Apply** to save your changes to the ZyXEL Device's run-time memory. The ZyXEL Device loses these changes if it is turned off or loses power, so use the Save Settings link in the navigation panel to save your changes to the non-volatile memory.

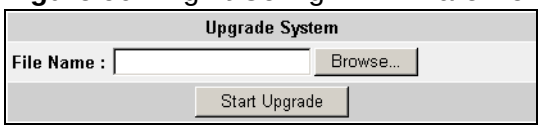
22.10 Upgrading the Firmware

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

Click **Mgmt Config** > **Firmware Download** to open the following screen.

Figure 90 Mgmt Config > Firmware Download



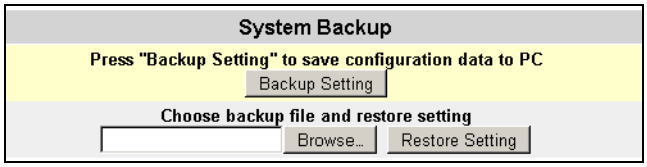
Type the path and file name of the firmware file you wish to upload to the MES-2110 in the **File Name** field or click **Browse** to locate it. Click **Start Upgrade** to load the new firmware.

After the firmware upgrade process is complete, the device will automatically restart. See the **System Details** > **Board Info.** screen to verify your current firmware version number.

22.11 Managing the Configuration File

Backing up your MES-2110 configurations allows you to create various “snap shots” of your device from which you may restore at a later date. Use this screen to back up or restore a configuration file. Click **Mgmt Config** > **Configuration File** to open the following screen.

Figure 91 Mgmt Config > Configuration File



Follow the steps below to back up the current MES-2110 configuration to your computer in this screen.

1 Click **Backup Setting**.

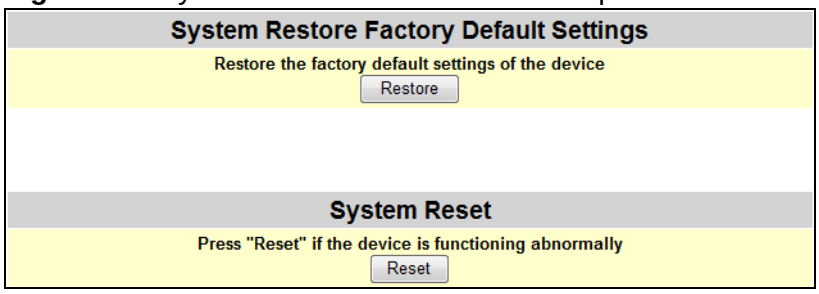
2 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

To restore a configuration file, type the path and file name of the configuration file you wish to restore in the field or click **Browse** to locate it. After you have specified the file, click **Restore Setting**. "config" is the name of the configuration file on the MES-2110, so your backup configuration file is automatically renamed when you restore using this screen.

22.12 Restarting the System

Click **System Restart Menu** > **Restart Option** to open the following screen. Use the Restore button to load the factory default settings, or use the Reset button to restart the system without physically turning the power off. It also allows you to load the factory default settings when you reboot.

Figure 92 System Restart Menu > Restart Option


System Restore Factory Default Settings
Restore the factory default settings of the device
Restore
System Reset
Press "Reset" if the device is functioning abnormally
Reset

23

Command Line Interface

23.1 Overview

This chapter introduces the MES-2110's command line interface (CLI).

23.1.1 Console Port Management

To manage the MES-2110 using the CLI:

1. Connect your computer to the console port on the MES-2110 using the appropriate cable.
2. Use terminal emulation software with the following settings:

SETTING	DEFAULT VALUE
Terminal Emulation	VT100
Baud Rate	9600
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

3. Press [ENTER] to trigger the login screen.

23.1.2 Logging in

Use the administrator password to log into the MES-2110. The default value administrator login username and password are: *admin* and *1234*.

The MES-2110 automatically logs you out of the management interface after five minutes of inactivity. If this happens, simply log back in again.

23.1.3 Using Shortcuts and Getting Help

This table identifies some shortcuts in the CLI, as well as how to get help.

Table 74 CLI Shortcuts and Help

COMMAND / KEY(S)	DESCRIPTION
↑↓ (up/down arrow keys)	Scrolls through the list of recently-used commands. You can edit any command or press [ENTER] to run it again.
[CTRL]+U	Clears the current command.
?	Displays the keywords and/or input values that are allowed in place of the ?. There are 2 types of help in the MES-2110: descriptive and parameter. **Descriptive help**: This type of help displays a short description of the command. To display descriptive help, simply type **command?** with no space between the command's final letter and the question mark. **Parameter help**: This type of help displays all available parameters for the command in question. To display parameter help, type **command ?** with a space between the command's final letter and the question mark. In some cases, commands do not have any parameters and typing this results in the command being carried out.
help	Displays the (full) commands that are allowed in place of help.

23.2 Saving Changes

In the MES-2110, whenever you make changes using the command line interface they are not saved by default.

To save your changes, you must use the following commands starting in Basic command mode (for details on this mode, see Section 23.5 on page 182):

```
MES-2110> enable
MES-2110# write memory
It takes a few moments to write memory...

MES-2110#
```

23.3 Logging Out

Enter `exit` to log out of the CLI while in Basic mode.

Table 75 Exit Command

COMMAND	DESCRIPTION
`exit`	Logs you out of the CLI while in Basic mode. If in any other mode, then this command returns you to the previous mode.

23.4 Command Modes

The MES-2110 segregates commands by command mode. Commands for a particular mode are only available once you set the device to that particular mode.

The following is list of available command modes.

Table 76 Basic Commands

MODE	TRIGGER	DESCRIPTION
Basic	Log in.	This is the default command line interface mode when you log into the device. Commands are restricted in this mode. See Section 23.5 on page 182 for details.
Privileged	While in Basic mode, type *enable* at the prompt and then press **[ENTER]**.	This mode a limited command set for configuring some of the MES-2110's features. See Section 23.6 on page 183 for details.
Configuration	While in Privileged mode: Type *configure terminal* at the prompt and then press **[ENTER]**.	This mode allows to you configure all of the MES-2110's advanced options. Configuration mode also has 3 ancillary modes: MVR, VLAN, and Interface. See Section 23.7 on page 186 for details.

23.5 Basic Commands

Basic commands are in all modes.

When in Basic mode, the command prompt is as follows:.

```
MES-2110>
```

The following is a list of available Basic commands:

Table 77 Basic Commands

COMMAND	DESCRIPTION
exit	In Basic mode, this disconnects you from the device (identical to logout). In other modes (such as Privileged), this returns you to the previous mode.
help	Lists available commands.
history	Displays a list of previously run commands.
logout	Disconnects from the device.
ping <-n count> <-l length> <-t> <-w timeout> <ip-address>	Pings the specied IP address. You can use the following parameters: **-n count**: Determines the number of echo requests to send. The default is 4. **-l length**: Adjusts the size of the ping packet by the number of specified bytes (64~8148). **-t**: Pings the specified host until the break (ESC) key is pressed. **-w timeout**: Adjusts the timeout duration for the ping packet in milliseconds. The default is 1,000 milliseconds.
show ip	Displays the device's network configuration.
show system-information	Shows the device's system configuration.

23.6 Privileged Command Mode

When in Privileged mode, the command prompt is as follows:.

```
MES-2110#
```

The following is a list of Privileged mode commands:

Table 78 Privileged Commands

COMMAND	DESCRIPTION
enable	Turns on Privileged mode commands.
disable	Turns off Privileged mode commands, returning the device to Basic mode.
copy config tftp <ip-address> <file-name>	Uploads a configuration file from the specified TFTP server's IP address.
copy firmware tftp <ip-address> <file-name>	Uploads a firmware file from the specified TFTP server's IP address.
copy syslog tftp <ip-address> <file-name>	Uploads a syslog file from the specified TFTP server's IP address.
copy tftp command-text <ip-address> <file-name>	Downloads a command file from the specified TFTP server's IP address.
copy tftp config <ip-address> <file-name>	Downloads a configuration filefrom the specified TFTP server's IP address.
copy tftp firmware <ip-address> <remote-file-name>	Downloads a firmware file from the specified TFTP server's IP address.
reset default	Resets the device to its factory default settings.
reset system	Resets the system.
show abnormal	Displays the abnormal traffic detection configuration.
show arp inspection <config|status>	Displays ARP inspection information. **config**: Displays the ARP inspection configuration file. **status**: Displays the ARP inspection records.
show bandwidth-control	Diplays the bandwidth control information.
show cable <all|port-number>	Displays the cable test results. Select all to view all test result or test by a specific port number.
show 8021p-priority	Displays the 8021p priority configuration for all ports.
show console-baudrate	Displays the baud rate of the console port.
show console-timeout	Displays the number of idle seconds allowed on the console port before the device automatically terminates the session.
show dhcp smart-relay	Displays DHCP smart relay information.
show dhcp snooping	Displays DHCP snooping information.

Table 78 Privileged Commands

COMMAND	DESCRIPTION
show dhcp static-binding	Displays the DHCP static binding table.
show dhcp dynamic-binding	Displays the DHCP dynamic binding table.
show dot1x global	Displays 802.1x global information.
show dot1x radius-server	Displays the 802.1x RADIUS server configuration.
show dot1x port-control	Displays the 802.1x port-control information.
show email-alarm	Displays the email configuration.
show frame	Displays the maximum frame size configuration.
show hdos	Displays the Denial-of-Service configuration.
show igmp	Displays the igmp configuration.
show interface	Display detailed port information for all ports.
show LACP	Displays LACP information.
show locked-mac	Displays the locked MAC address learning status.
show logins	Displays a list of recent logins.
show loop	Displays the loop detection configuration.
show mac	Displays the MAC table.
show mac-aging-time	Displays the MAC aging time.
show mac-filter-table	Displays the MAC filter table.
show mac-limit	Displays the MAC limit table.
show mirror	Displays the mirror configuration.
show mvr	Displays multicast status, including the port number, VLAN ID and multicast group members on the switch. Optionally, displays the type of each multicast VLAN.
show priority-override	Displays the priority override status table.
show qinq-sp-tpid	Displays the Server Provider Tag Prototol Identifier.
show qos priority-mode	Displays QoS priority-mode and IP-over-tag settings.
show qos default-priority-queue	Displays the QoS port priority.
show qos tag-priority-queue	Displays the QoS tag priority.
show qos ip-tos-pri-queue	Displays the QoS IP-TOS priority to queue mapping.
show qos schedule	Displays the QoS schedule type.
show rmon port [+n | all]	Displays the device's RMON information. **+n**: Enter plus sign followed by port number to display just that port's information. For example, **show rmon port +1**. You can also chain multiple port numbers together, such as **show rmon port +1+2+6** (which displays information for just ports 1, 2, and 6). **all**: Displays RMON information for all ports.

Table 78 Privileged Commands

COMMAND	DESCRIPTION
show rstp	Displays the RSTP configuration.
show sfp ddmi port <port-number>	Displays the SFP fiber port DDMI information for the specified port.
show sfp serial-no port <port-number>	Displays the SFP serial number for the specified port.
show sfp vendor port <port-number>	Displays the SFP vendor name for the specified port.
show snmp	Displays the snmp configuration.
show sntp	Displays the SNTP configurations.
show sntp-timezone	Displays a list of time zones and their GMT offset.
show storm-control	Displays the storm control configuration.
show syslog [<begin:end>]	Displays all syslog messages. You can also specify a range of syslog messages. **begin**: Enter the first syslog message to display. **end**: Enter the last syslog message to display.
show syslog-config	Displays the syslog configuration.
show version	Displays the system version.
show vlan port-base	Displays the port-base VLAN.
show vlan stacking	Displays the VLAN stacking status.
show vlan tag-base management-VLAN	Displays the VLAN for the management switch.
show vlan tag-base vlan-id	Displays the tag-base VLAN ID.
show vlan tag-base port-info	Displays the tag-base port information.
show vlan tag-base vlan-table	Displays tag-base VLAN table.
show vlan type	Displays the VLAN type.
write memory	Saves the current configuration, including all changes made since the last save, to flash. Note: You must use this command to permanently save any changes you make while using the MES-2110 command line interface.

23.7 Configuration Mode

When in Configuration mode, the command prompt is as follows:.

```
MES-2110(config)#
```

There are 3 additional ancillary available while in Configuration mode. They are:

Table 79 Basic Commands

ANCILLARY	TRIGGER	DESCRIPTION
MVR	While in Configuration mode: Type *mvr <1-4094>* (where 1-4094) is the MVR ID ranging from 1 to 4094) at the command line prompt and then press **[ENTER]**. If no MVR exists, then this creates one for you.	This mode allows to configure the MES-2110's MVR IDs and their associated options. See Section 23.8 on page 195 for details.
VLAN	While in Configuration mode: Type *vlan <1-4094>* (where 1-4094 is a VLAN ID ranging from 1 to 4094) at the command line prompt and then press **[ENTER].** If no VLAN ID exists, then this creates one for you.	This mode allows you to configure the MES-2110's VLAN IDs and their associated options. See Section 23.9 on page 197 for details.
Interface	While in Configuration mode: Type *interface <port>* (where port is a port number) at the command line prompt and then press **[ENTER]**	This mode allows you to configure the MES-2110's port interfaces and their associated options. See Section 23.10 on page 198 for details.

The following is a list of baseline Configuration mode commands:

Table 80 Configuration Mode Commands

COMMAND	DESCRIPTION
`configure terminal`	Toggles the Configuration mode, but only if you are first in Privileged mode.
`abnormal detection <enable|disable>`	Enables or disables abnormal traffic detection.
`abnormal duration <1-60>`	Sets the abnormal traffic detection duration in seconds (1-60).
`abnormal interval <1-600>`	Sets the protection interval in seconds (1-600).
`abnormal permanently <yes|no>`	Blocks any port permanently when abnormal traffic is detected and this option is set to **yes**.
`abnormal threshold <2000-20000>`	Sets the threshold of traffic detection in packets per second (2000-20,000).

Table 80 Configuration Mode Commands

COMMAND	DESCRIPTION
`arp inspection enable`	Enables ARP inspection. Note: You must still enable ARP inspection on specific VLAN and specify trusted ports if you use this option.
`arp inspection vlan <1-4094>`	Sets the ARP inspection VLAN ID.
`arp inspection vlan-mode <all|fixed>`	Sets the ARP inspection VLAN mode.
`arp inspection mac-filter-aging <0-10080>`	Specifies how long (in minutes) MAC address filters remain in the device after it identifies an unauthorized ARP packet. The device automatically deletes the MAC address filter afterwards. Use '0' in the parameter field to make it permanent.
`console-baudrate <9600|19200|38400>`	Sets the console port's baudrate.
`console-timeout <0|10~3600>`	Sets the console timeout in seconds. **0**: Sets the console to never timeout **10~3600**: Sets the console timeout in seconds (minimum 10 seconds, maximum 3600 seconds, default 300 seconds.)
`dhcp binding <mac-address> <ip-address> <port> <vlan-id>`	Adds the specified MAC address, IP address, port numer, and VLAN ID to the DHCP snooping static binding table.
`dhcp client`	Enables DHCP client.
`dhcp option-information <remote-id>`	Sets the DHCP Option Remote ID. **remote-id**: Enter a maximum of 64 characters.
`dhcp smart-relay enable`	Enables DHCP smart relay.
`dhcp smart-relay exlude-vlan <1-4094>`	Sets the DHCP smart relay to exlude the specified VLAN.
`dhcp smart-relay helper-address <ip-address>`	Sets the IP address of the DHCP server. **ip-address**: Enter the IP address of the remote server.
`dhcp smart-relay option`	Allows the device to add DHCP relay agent information.
`dhcp snooping enable`	Enables DHCP snooping.
`dhcp snooping vlan <1-4094>`	Sets the DHCP snooping VLAN ID.
`dhcp snooping vlan-mode <all|fixed>`	Sets the DHCP snooping VLAN mode. **all**: Enter this to have the device enable DHCP snooping on all VLANs dynamically. **fixed**: Enter this to specify which VLANS can be enabled with DHCP snooping.
`dhcp snooping option`	Allows the device to add the DHCP option.

Table 80 Configuration Mode Commands

COMMAND	DESCRIPTION
dot1x enable	Enables 802.1x on the device.
dot1x reauth-max <1~10>	Sets the maximum number of times re-authentication can be used (1~10). The default is 2 times. This kind of authentication method is port-based.
dot1x guest-vlan <1-4094>	Sets the VLAN ID of the guest VLAN. This must be an existing VLAN.
dot1x radius-server server-ip <ip-address>	Sets the RADIUS server's IP address.
dot1x radius-server shared-secret <string>	Sets the password for RADIUS server access. **string**: Enter a maximum of 29 characters.
dot1x radius-server server-udp-port <1-65535>	Sets the UDP port number of the RADIUS server. The default is 1812.
dot1x radius-server accounting-port <1-65535>	Sets the accounting port of the RADIUS server. The default is 1813.
dot1x radius-server timeout <1-300>	Sets the timeout period of the RADIUS server. The default is 30.
email-alarm disable	Disables the email alarm. This is the default.
email-alarm enable	Enables the email alarm.
email-alarm from <string|cr>	Sets the email alarm's "from" field to the specified string. **string**: Enter up to 63 characters. **cr**: Leave this blank and press the [Enter] key to clear the email-alarm from setting.
email-alarm server <ip-address>	Sets the email alarm's server to the specified IP address.
email-alarm to [<id> <string> <enable|disable>] | [<id>]	Sets the email alarm's "to" field. **id**: Enter an ID number for this recipent (1~5). If you enter just the ID and no other paramters (**string** or **enable|disable**), then this setting is cleared for that ID. **string**: Enter the recipient's email address. **enable|disable**: Select whether to enable this recipient or disable it. When disabled, no alarm emails are sent to that recipient.
email-alarm type <coldstart|warmstart|rj45up|rj45down|gigeup|gigedown|confchange|newroot1d|topochange1d|arpinspectionover> <enable|disable>	Sets the email alarm type. When one of these events occurs and you have enabled that email alarm type, the device sends out an alarm email. You must configure each event individually. For example: **email-alarm type coldstart enable**. This enables it for the coldstart event. If you want to also enable it for the warmstart event, you must configure it separately: **email-alarm type warmstart enable**.

Table 80 Configuration Mode Commands

COMMAND	DESCRIPTION
erase-mac-table	Erases all dynamic MAC entries from the MAC table.
frame-size <1522|1632>	Sets the frame size. The default is 1632.
gateway <ip-address>	Sets the gateway IP address.
hdos ip <index> <ip-address>	Sets the acceptable IP address for Host Denial of Service (DoS) protection. **index**: Enter an index number (1-5). **ip-address**: Enter an IP address to associate with an index number.
hdos ip-enable <index> <enable|disable>	Enables or disables an individual IP address for Host Denial of Service (DoS) protection. **index**: Enter an index number (1-5). **enable|disable**: Enable or disable the IP address associated with this index number.
hdos protection <enable|disable>	Enables or disables the Host Denial of Service (DoS) protection service.
igmp immediate-leave <port-list>	Sets the port list for IGMP immediate-leave.
igmp query-mode <auto|disable>	Sets the IGMP query mode.
igmp snooping	Enables IGMP snooping.
igmp static <port-list>	Sets the IGMP static port list.
igmp vlan <1-4094>	Specifies the VLANs on which to perform IGMP snooping if the mode is fixed.
igmp vlan-mode <auto|fixed>	Specifies how the VLANs snooped by the device select IGMP packets. **auto**: The device learns multicast group membership on any VLAN. It drops a.ny IGMP control messages on other VLANs after it reaches this maximum number (auto mode). **fixed**: The device only learns multicast group membership on specified VLAN(s). It drops any IGMP control messages for any unspecified VLANs (fixed mode).
igmp vlan-query-mode <vlan-id> <auto|disable>	Specifies the query mode for the specified VLAN.
ip <ip-address>	Sets the IP address of the device to the one specified.
lacp group <group> <lacp|static>	Sets the specified trunk group to LACP or static.
lacp hash-mode <xor|lookup>	Sets the hash mode for trunk load balancing selection. **xor**: Select this XOR the lower 3 bits of the DA and SA frames together. **lookup**: Select this to use the lookup table.

Table 80 Configuration Mode Commands

COMMAND	DESCRIPTION
lacp port <port> <active|passive>	Sets the LACP port state to active or passive.
lacp priority <0-65535>	Sets the system priority for LACP.
lacp restart	Stores the LACP configurations and then restarts them.
lacp trunk <group number> member <port num> <port num> <port num> ...	Sets the trunk control configuration.
logins	Modifies the login account. This prompts you to enter the old username and password; to create a new username and password; then set the login account's read/ writer permissions.
loop detection <enable|disable>	Enables or disables loop detection.
loop mac <mac-address>	Sets the loop detection test frame MAC address.
loop port <id> <enable|disable>	Enables or disables individual port loop detection.
mac-aging-time <1-255>	Sets the MAC aging time configuration. The default is 19 (which converts to 304 seconds). To determine the number of seconds, multiply the MAC aging time value you enter by 16.
mac-filter add-allow-mac <mac-address> <port id> <priority> <override-enable|override-disable>	Sets the static unicast MAC configuration.
mac-filter add-deny-mac <mac-address>	Adds a specified MAC address to the deny MAC configuration.
mac-filter delete <mac-address>	Deletes a static unicast MAC configuration.
mac-limit <enable|disable>	Enables or disables MAC-limit configuration.
mirror mode <all|disable>	Sets the mirror mode.
mirror monitoring-port <port-id>	Sets the mirror monitoring port.
netmask <netmask>	Sets the netmask.
no arp inspection enable	Disables ARP inspection.
no arp inspection mac-filter <mac-address>	Deletes the specified MAC address from the ARP inspection filter.
no arp inspection vlan <1-4094>	Disables ARP inspection on the specified VLAN.
no dhcp client	Disables the DHCP client.
no dhcp binding mac <mac-address>	Deletes the DHCP snooping static binding table by MAC address.
no dhcp binding ip <ip-address>	Deletes the DHCP snooping static binding table by IP address.
no dhcp binding port <port-id>	Deletes the DHCP snooping static binding table by port.
no dhcp binding vid <vlan-id>	Deletes the DHCP snooping static binding table by VLAN ID.
no dhcp smart-relay enable	Disables DHCP smart relay.

Table 80 Configuration Mode Commands

COMMAND	DESCRIPTION
no dhcp smart-relay option	Disables the DHCP smart relay option.
no dhcp smart-relay vlan <cr|range>	Sets the DHCP smart relay to exclude VLANs. **cr**: Leave this field blank and press [Enter] to use the default setting. **range**: Specify a range of VLAN IDs.
no dhcp snooping enable	Disables DHCP snooping.
no dhcp smart-relay exlude-vlan <1-4094>	Sets the DHCP smart relay to include the previously excluded specified VLAN.
no dhcp snooping option	Disables the DHCP snooping option.
no dhcp snooping vlan <1-4094>	Disables the specified DHCP snooping VLAN ID.
no dot1x global	Stops 802.1x running globally
no dot1x guest-vlan	Disables Guest VLAN.
no gateway	Sets the device's default gateway.
no igmp immediate-leave	Sets IGMP fast leave to its default value.
no igmp query-mode <vlan-id>	Sets IGMP query mode to its default type for the specified VLAN ID.
no igmp snooping	Disables IGMP snooping.
no igmp static	Disables the IGMP static port.
no igmp vlan <1-4094>	Disables IGMP VLAN for the specified VLAN ID.
no ip	Sets the device to its default IP address. Note: You cannot change the device's IP address over Telnet.
no lacp	Disables LACP.
no logins	Resets the login password to NULL.
no mvr <1-4094>	Removes an MVR configuration from the specified VLAN.
no netmask	Sets the default netmask.
no spanning-tree	Disables the spanning tree.
no trunk <group-id>	Disables the trunk group.
no vlan <2-4094>	Deletes the static VLAN entry.
no vlan-stacking	Disables VLAN stacking.
qinq-sp-tpid <tpid>	Sets the SP TPID. SP TPID is a standard Ethernet type code identifying the frame and indicating whether the frame carries IEEE 802.1Q tag information. **tpid**: Enter the Server Provider Tag Protocol Identifier. This can be a four-digit hexadecimal number from 0000 to ffff. The default is 9100.
qos schedule all_high_before_low	Sets the QoS schedule to all high before low.
qos schedule weighted_round_robin	Sets the QoS to weighted round_robin.

Table 80 Configuration Mode Commands

COMMAND	DESCRIPTION
qos ip-dscp-pri-queue <0~63> <low|normal|preferred|high>	Sets the QoS IP IP-DSCP Priority to queue mapping. The default is low.
qos tag-pri-queue <0-7> <low|normal|preferred|high>	Set the QoS tag priority to queue mapping.
rmon clear	Clears the RMON information for ports 1~10.
snmp contact <contact-name>	Sets the SNMP system contact name. **contact-name**: Enter up to 80 characters.
snmp getcommunity <community-name>	Sets the SNMP GET community. **community-name**: Enter up to 30 characters. Note: Only for SNMP v2c or lower.
snmp location <location-name>	Sets the SNMP system location. **location-name**: Enter up to 80 characters.
snmp setcommunity <community-name>	Sets the SNMP SET community. **community-name**: Enter up to 30 characters. Note: Only for SNMP v2c or lower.
snmp trapcommunity <index> <community-string>	Sets the SNMP trap community. **index**: Enter an index number (1~5). **community-string**: Enter up to 30 characters.
snmp trapenable <index> <enable|disable>	Enables the SNMP trap. **index**: Enter an index number (1~5).
snmp trapip <index> <ip-address>	Sets the IP addresses of up to 5 SNMP managers to receive SNMP traps. **index**: Enter an index number (1~5).
sntp <enable | disable>	Enables and disables SNTP support.
sntp-NTP-primary-server <ip address>	Set SNTP primary server's IP address.
sntp-NTP-secondary-server <ip address>	Set SNTP secondary server's IP address.
sntp poll_interval <value>	Sets the interval in specified hours between SNTP requests.
sntp time <yyyy:mo:dd:hh:mm:ss>	Sets the local time by year (yyyy), month (mm), day (dd), hour (hh), minutes (mm), and seconds (ss).
sntp timezone <+hh.mm | -hh.mm>	Sets the timezone offset. **+hh.mm**: Increases the timezone offset by the specified hours (hh) and minutes (mm). **-hh.mm**: Increases the timezone offset by the specified hours (hh) and minutes (mm).

Table 80 Configuration Mode Commands

COMMAND	DESCRIPTION
sntp daylightsavingstart <mo.dd>	Sets the daylight savings time start date for the specified month (mo) and day (dd).
sntp daylightsavingend <mo.dd>	Sets the daylight savings time end date for the specified month (mo) and day (dd).
sntp daylightsaving <enable | disable>	Enables or disables daylight savings time.
spanning-tree enable	Enables RSTP.
spanning-tree forward-delay <4-30>	Sets the RSTP forward delay. The default is 15.
spanning-tree hello-time <1-10>	Sets the RSTP hello time. The default is 2.
spanning-tree maximum-age <6-40>	Sets the RSTP maximum age. The default is 20.
spanning-tree priority <0-61440>	Sets the RSTP switch priority the default is 32768.
syslog enable	Enables syslog support.
syslog disable	Disables syslog support.
syslog clear	Clears all data out of the syslog.
system-name <string>	Sets the system name to the specified string. **string**: Enter up to 30 characters.
vlan-stacking	Enables VLAN stacking on the device.
vlan-type <802.1q | port-base>	Configures VLAN type.

23.7.1 IGMP Snooping Example

This example enables IGMP snooping, then sets the query mode to “Auto” and port #10 to static..

```
MES-2110(config)# igmp snooping
MES-2110(config)# igmp query-mode auto
MES-2110(config)# igmp static 10
```

23.7.2 RADIUS Configuration Example

This example sets up one RADIUS server (172.16.10.10) and a shared secret key (“hello”) for authentication.

```
MES-2110# configure terminal
MES-2110(config)# vlan 99
MES-2110(config-vlan)# exit
MES-2110(config)# dot1x enable
MES-2110(config)# dot1x radius-server server-ip 172.16.10.10
MES-2110(config)# dot1x radius-server shared-secret hello
MES-2110(config)# dot1x guest-vlan 99
MES-2110(config)# exit
MES-2110(config)# interface port-channel 1
MES-2110(config-interface)# dot1x guest-vlan enable
MES-2110(config-interface)# end
MES-2110# show dot1x radius-server

Server IP Address : 172.16.10.10
Shared Key : hello
Sever Port Number : 1812
Accounting Port Number: 1813
Sever Time-out(sec) : 30
MES-2110# show dot1x global
802.1x protocol: Enabled
reauth-max: 2
Guest VLAN VID: 99

MES-2110# show dot1x port-control
802.1x Port-control Parameters
Guest VLAN VID:99
Port Active Reauthentication ReauthPeriod GuestVlan
  1    No         Off         3600 (sec)     Yes
  2    No         Off         3600 (sec)     No
  3    No         Off         3600 (sec)     No
  4    No         Off         3600 (sec)     No
  5    No         Off         3600 (sec)     No
  6    No         Off         3600 (sec)     No
  7    No         Off         3600 (sec)     No
  8    No         Off         3600 (sec)     No
  9    No         Off         3600 (sec)     No
 10    No         Off         3600 (sec)     No
```

23.8 MVR Mode

This is an ancillary mode of Configuration mode. You must be in Configuration mode for these commands to work.

When in MVR-Configuration mode, the command prompt is as follows:.

```
MES-2110(config-mvr)#
```

The following is a list of available MVR-Configuration mode commands:

Note: These commands only apply to the MVR ID specified when you enter MVR-Configuration mode.

Table 81 MVR-Configuration Mode Commands

COMMAND	DESCRIPTION
`mvr <1-4094>`	Enters MVR (multicast VLAN relay) configuration mode for the specified MVR, creating the MVR if necessary. Note: You must be in Configuration mode for this command to work.
`group <group-id> <start-address> <n>`	Sets the multicast group range for the current MVR group. **group-id**: Enter 1-255 characters for the group identification. **start-address**: Enter the start IP address for the multicast range of this group. **n**: Enter the number of additional addresses to generate based on the start address for the multicast range of this group.
`inactive`	Disables the MVR settings for the current MVR group.
`no inactive`	Enables the 'no' settings for the current MVR group.
`no receiver-port <port-list>`	Disables the receiver port(s) for the current MVR group.
`no source-port <port-list>`	Disables the source port(s) for the current MVR group.
`no tagged <port-list>`	Sets the untag port numbers for the current MVR group.
`no group <cr|group-id>`	Removes all or specified MVR group settings for the current MVR group. **cr**: Leave this field blank and press [Enter]. **group-id**: Enter the group ID to remove.

Table 81 MVR-Configuration Mode Commands

COMMAND	DESCRIPTION
`mode <dynamic|compatible>`	Sets the MVR mode to dynamic or compatible for the current MVR group.
`name <name>`	Sets the current MVR group name for identification purposes. **name**: Enter 1-30 characters.
`query-mode <auto|disable>`	Sets the query mode of the current MVR group.
`receiver-port <port-list>`	Sets the receiver port(s) for the current MVR group. An MVR receiver port can only receive multicast traffic in a multicast VLAN.
`source-port <port-list>`	Sets the source port(s) for the current MVR group. An MVR source port can send and receive multicast traffic in a multicast VLAN.
`tagged <port-list>`	Sets the port(s) to VLAN tags for the current MVR group.

23.8.1 MVR Command Example

This example configures MVR in the following ways:

1. Enters MVR mode. This creates a multicast VLAN with the name StreamVlan and the multicast VLAN ID of 100.
2. Specifies source port 9 for the multicast group.
3. Specifies receiver ports 1-4 and 10 for the multicast group.
4. Specifies dynamic mode for the multicast group.
5. Sets the ports 9 and 10 to tag VLAN IDs.
6. Configures MVR multicast group addresses 227.3.3.1 through 227.3.3.10 for multicast group ID 1.

```
MES-2110(config)# mvr 100
MES-2110(config-mvr)# no inactive
MES-2110(config-mvr)# name StreamVlan
MES-2110(config-mvr)# mode dynamic
MES-2110(config-mvr)# receiver-port 1,2,3,4,10
MES-2110(config-mvr)# source-port 9
MES-2110(config-mvr)# tagged 9,10
MES-2110(config-mvr)# group 1 227.3.3.1 10
```

23.9 VLAN Mode

This is an ancillary mode of Configuration mode. You must be in Configuration mode for these commands to work.

When in VLAN-Configuration mode, the command prompt is as follows:.

```
MES-2110(config-vlan)#
```

The following is a list of available VLAN-Configuration mode commands:

Note: These commands only apply to the VLAN ID specified when you enter VLAN Configuration mode.

Table 82 VLAN Mode Commands

COMMAND	DESCRIPTION
vlan <1-4094>	Enters VLAN Configuration mode for the specified VLAN ID. If no VLAN IDs exist, then this creates the specified ID.
manage	Sets the current VLAN as a management VLAN.
member <port-list>	Specifies the ports that are members of the current VLAN group.
non-member <port-list>	Specifies the ports that are excluded from the current VLAN group.
tagging <port-list>	Specifies the ports in the current VLAN group for which you want outgoing frames tagged.
untagging <port-list>	Specifies the ports in the current VLAN group for which you do not want outgoing frames tagged.
use-vid-priority <yes|no>	Select yes to enable VID priority for the current VLAN group, or **no** to disable it.
vid-priority <0~7>	Sets the VID priority (0~7).

23.9.1 VLAN ID Priority Example

This example assigns port 1 as a tagged port for VLAN 1 and sets the priority of all incoming packets from VLAN 1 to priority 3.

```
MES-2110> enable
MES-2110# configure terminal
MES-2110(config)# vlan 1
MES-2110(config-vlan)# tagging 1
MES-2110(config-vlan)# vid-priority 3
MES-2110(config-vlan)# use-vid-priority yes
MES-2110(config-vlan)# exit
MES-2110(config)# interface port-channel 1
MES-2110(config-interface)# vid-pri-override enable
MES-2110(config-interface)# exit
MES-2110(config)# exit
MES-2110# show priority-override

port    vid-pri-override     da-pri-override     sa-pri-override
================================================================
 01        enabled              disabled            disabled
 02        disabled             disabled            disabled
 03        disabled             disabled            disabled
 04        disabled             disabled            disabled
 05        disabled             disabled            disabled
 06        disabled             disabled            disabled
 07        disabled             disabled            disabled
 08        disabled             disabled            disabled
 09        disabled             disabled            disabled
 10        disabled             disabled            disabled

MES-2110# show vlan tag-base vlan-table

                                                      1 (M:member, U:untag)
No.    VLAN-ID    Priority    Pri-override    1234567890 (T:tag, -:nomember)
=========================================================
   1   1              3            Yes        TUUUUUUUUU
   2   24             0            No         ----------
MES-2110#
```

23.10 Interface Mode

This is an ancillary mode of Configuration mode. You must be in Configuration mode for these commands to work.

When in Interface-Configuration mode, the command prompt is as follows:.

```
MES-2110(config-interface)#
```

Note: These commands only apply to the ports specified when you enter Interface Configuration mode.

Table 83 Interface Mode Commands

COMMAND	DESCRIPTION
`interface port-channel <port-list>`	Enters Interface Configuration mode for the specified port(s).
`abnormal-detection-enable`	Enables port detection for the current port(s).
`active`	Enables the current port(s).
`arp-inspection-trust`	Enables ARP inspection trust for the current port(s). When enabled, the device does not discard ARP packets on trusted ports.
`auto-negotiation`	Enables auto-negotiation for the current port(s).
`bandwidth-limit egress <cr>| <low|medium|high> <rate>`	Sets the egress rate for the current port(s). **cr**: Press **[ENTER]** without entering any other parameters to enable egress bandwidth control on the current port(s). **low**: 64K~960K (64..960) in 64k steps. **medium**: 1~100M (1..100) in 1M steps. **high**: 100~1000M (110..1000) in 10M steps.
`bandwidth-limit ingress <low|medium|high> <rate>`	Sets the ingress rate for the current port(s). **cr**: Press **[ENTER]** without entering any other parameters to enable egress bandwidth control on the current port(s). **low**: 64K~960K (64..960) in 64k steps. **medium**: 1~100M (1..100) in 1M steps. **high**: 100~1000M (110..1000) in 10M steps.
`bpdu-mode <on|off|tunnel>`	Sets the BPDU packet process mode for the current port(s).
`da-pri-override <enable|disable>`	Sets the destination MAC priority override for the current port(s).
`dhcp snooping trust`	Sets DHCP snooping trust for the current port(s). Trusted ports are connected to DHCP servers or other switches, and the device discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.
`egress-set <port-list>`	Sets the outgoing traffic port list for a port-base VLAN for the current port(s).
`flow-control`	Enables interface flow control for the current port(s).

Table 83 Interface Mode Commands

COMMAND	DESCRIPTION
frame-type <fallback|check|secure>	Sets the port frame type for the current port(s). You can choose to accept both non-member and untagged incoming frames (fallback), just untagged incoming frames (check) or drop all non-member and untagged incoming frames on a port (secure). **fallback**: Accepts incoming frames (nonmember forward/untag forward). **check**: Accepts incoming frames (nonmember drop/untag forward). **secure**: Accepts incoming frames (nonmember drop/untag drop).
isolate	Isolates the specified prots. Isolated ports belonging to the same VLAN do not communicate with each other.
lock-mac	Locks the MAC configuration for the current port(s).
mac-limit action <enable|disable>	Enables or disables the MAC limit for the current port(s).
mac-limit quantity <1-20>	Sets the MAC limit quantity for the current port(s).
mirror	Enables port mirroring for the current port(s).
name <string>	Sets a name for the port for the current port(s). **string**: Enter up to 15 characters.
no abnormal	Disables individual port detection for the current port(s).
no active	Disables the current port(s).
no arp-inspection-trust	Disables ARP inspection trust for the current port(s).
no bandwidth-limit egress	Disables egress rate for the current port(s).
no bandwidth-limit ingress	Disables ingress rate for the current port(s).
no dhcp snooping trust	Disables DHCP snooping trust for the current port(s).
no flow-control	Disables flow control on the interface for the current port(s).
no auto-negotiation	Disables auto-negotiation. for the current port(s).
no isolate	Disables port isolation for the current port(s).
no lock-mac	Disables MAC locking for the port for the current port(s).
no mirror	Disables port mirroring for the current port(s).
no broadcast-limit	Disables the broadcast packet limit for the current port(s).

Table 83 Interface Mode Commands

COMMAND	DESCRIPTION
no multicast-limit	Disables the multicast packet limit for the current port(s).
no dlf-limit	Disables the DLF packet limit for the current port(s).
no dot1x port-control	Disables port control of 802.1x for the current port(s).
no dot1x guest-vlan	Disables guest VLAN for the current port(s).
no dot1x reauth	Disables reauthentication of 802.1x for the current port(s).
8021p-priority <0-7>	Sets default ingress priority to use when no priority information avilable for the current port(s).
pvid <1-4094>	Sets the PVID for the current port(s).
qos-priority-mode <default|tag|ip|ip&tag>	Sets the QoS priority mode for the current port(s). **default**: Port Priority. **tag**: IEEE Tagged Frame Priority. **ip**: IPv4 and IPv6 Frame Priority. **ip&tag**: IPv4 and IPv6 with IEEE Tagged Frame Priority.
qos-ipdscp-over-tag <enable|disable>	Sets the QoS ipdscp over tag priority for the current port(s).
dot1x reauth-period <1-999999>	Set reauthentication period for the current port(s). The default is 3600.
dot1x enable	Enable 802.1x port control for the current port(s).
dot1x reauth enable	Enable 802.1x reauthentication for the current port(s).
dot1x guest-vlan enable	Enables guest VLAN for the current port(s).
rstp-edge <on|off>	Sets the RSTP port edge for the current port(s).
rstp-p2p <auto|on|off>	Sets the RSTP port point-to-point (p2p) option for the current port(s).
rstp-path-cost <0-65535>	Sets the RSTP port path cost for the current port(s). The default is 1000M=4, 100M=19.
rstp-priority <0-255>	Sets the RSTP port priority for the current port(s). The default is 128.
sa-pri-override <enable|disable>	Sets the source MAC priority override for the current port(s).
speed-duplex <10f|10h|100f|100h|1000f>	Sets the duplex and speed mode for the current port(s).
sfp-speed <100|1000|1000-no-auto>	Sets the SFP fiber speed for the current port(s).

Table 83 Interface Mode Commands

COMMAND	DESCRIPTION
`storm-control broadcast-limit [cr | <low|medium|high> <rate>]`	Sets the broadcast storm control for the current port(s). **cr**: Enter nothing for this field and just press [Enter] to enable broadcast packet limits on the current port(s). **low**: 64K~960K (64..960) in 64k steps. **medium**: 1~100M (1..100) in 1M steps. **high**: 100~1000M (110..1000) in 10M steps.
`storm-control multicast-limit [cr | <low|medium|high> <rate>]`	Sets the multicast storm control for the current port(s). **cr**: Enter nothing for this field and just press [Enter] to enable multicast packet limits on the current port(s). **low**: 64K~960K (64..960) in 64k steps. **medium**: 1~100M (1..100) in 1M steps. **high**: 100~1000M (110..1000) in 10M steps.
`storm-control dlf [cr |<low|medium|high> <rate>]`	Sets the DLF storm control for the current port(s). **cr**: Enter nothing for this field and just press [Enter] to enable DLF packet limits on the current port(s). **low**: 64K~960K (64..960) in 64k steps. **medium**: 1~100M (1..100) in 1M steps. **high**: 100~1000M (110..1000) in 10M steps.
`vid-pri-overide <enable|disable>`	Enables or disables the VLAN ID priority override for the current port(s).
`vlan-stacking role <normal|access|tunnel>`	Sets the VLAN stacking port roles of the current port(s.) **normal**: The device ignores frames received (or transmitted) on this port with VLAN stacking tags. **access**: The device adds the SP TPID tag to all incoming frames received on this port. **tunnel**: Use this for egress ports at the edge of the service provider's network. Note: In order to support VLAN stacking on a port, the port must allow frames of 1526 bytes (1522 bytes + 4 bytes for the second tag) to pass through it.

Table 83 Interface Mode Commands

COMMAND	DESCRIPTION
`vlan-stacking SPVID <1-4094>`	Sets the service provider VLAN ID of the current port(s).
`vlan-stacking priority <0-7>`	Sets the priority (0-7) of the current port(s) in VLAN stacking.

23.10.1 Untrusted ARP Inspection Example

This example assigns port 1 to 8 as untrusted for ARP inspection, and displays whether the device's ports have a trusted or untrusted status. Generally if you want to enable ARP inspection on the device you also have to enable DHCP snooping first to build a binding table.

```
MES-2110(config)# dhcp snooping enable
MES-2110(config)# dhcp snooping vlan-mode all
MES-2110(config)# arp inspection enable
MES-2110(config)# arp inspection vlan-mode all
MES-2110(config)# interface port-channel 1,2,3,4,5,6,7,8
MES-2110(config-interface)# no arp-inspection-trust
MES-2110# show arp inspection config
ARP Inspection is enabled
ARP Inspection MAC-Filter-Aging-Time : 5(min)
ARP Inspection VLAN Mode : All VLAN
ARP Inspection VLAN :

Port       ARP-Inspection
--------------------------
01             untrust
02             untrust
03             untrust
04             untrust
05             untrust
06             untrust
07             untrust
08             untrust
09             trust
10             trust
```

23.10.2 Outgoing Traffic Bandwidth Limit Example

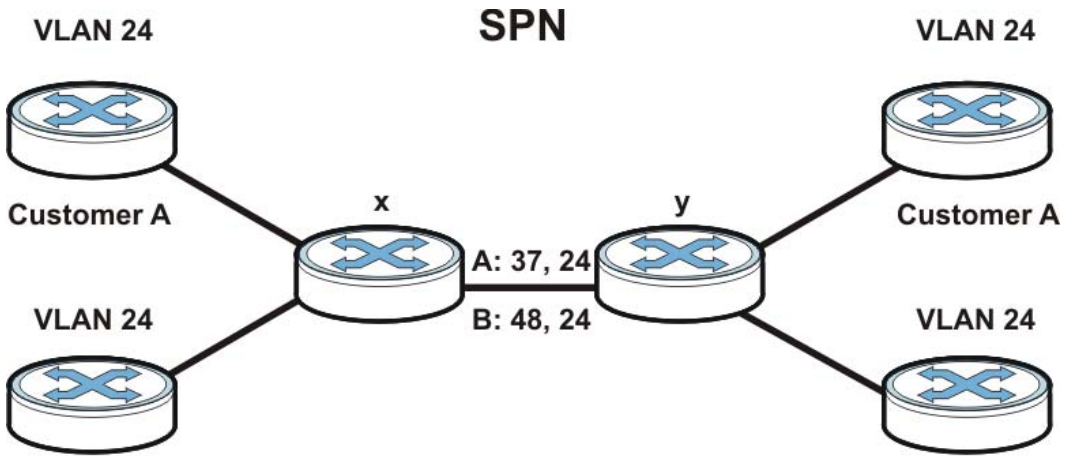
This example sets the outgoing traffic bandwidth limit to 1 Mbps for port 2.

```
MES-2110# configure terminal
MES-2110(config)# interface port-channel 2
MES-2110(config-interface)# bandwidth-limit egress medium 1
MES-2110(config-interface)# bandwidth-limit egress
```

23.10.3 Frame Tagging Examples

In the following example, both A and B are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer A and tag 48 to distinguish customer B at edge device x and then stripping those tags at edge device y as the data frames leave the network.

Figure 93 Frame Tagging Example



This example shows how to configure ports 1 and 2 on the switch to tag incoming frames with the service provider's VID of 37 (ports are connected to customer A network). This example also shows how to set the priority for ports 1 and 2 to 3.

```
MES-2110(config)# vlan-stacking
MES-2110(config)# interface port-channel 1,2
MES-2110(config-interface)# vlan-stacking role access
MES-2110(config-interface)# vlan-stacking spvid 37
MES-2110(config-interface)# vlan-stacking priority 3
MES-2110(config-interface)# exit
MES-2110(config)# exit
MES-2110# show vlan stacking

VLAN Stacking:Enabled
SP TPID:0x9100
Port       Role       SPVID       Priority
-----------------------------------------
1          Access        37              3
2          Access        37              3
3          Normal         1              0
4          Normal         1              0
5          Normal         1              0
6          Normal         1              0
7          Normal         1              0
8          Normal         1              0
9          Normal         1              0
10         Normal         1              0
```

This example applies only to switches that support the SVLAN feature. It shows how to configure both port 1 (connected to customer A) and port 2 (connected to customer B) as the ingress ports (access ports) and port 10 as the egress port (tunnel port) on the switch (edge device x of the service provider's network). Incoming frames received on port 1 and 2 are tagged with the ingress ports' SP VID 37 and 48 respectively before the switch forwards them to port 10.

The ingress ports (port 1 and 2) and the egress port (port 10) should be in the same static VLAN (customer VLAN) to communicate with each other. This example also shows how to configure service provider's VLANs 37 and 48 in the switch's SVLAN table. The switch checks the incoming frames received on the tunnel port (port 10) and drops the frames whose SPVID is not in the SVLAN table.

```
MES-2110# configure terminal
MES-2110(config)# interface port-channel 1
MES-2110(config-interface)# vlan-stacking role access
MES-2110(config-interface)# vlan-stacking SPVID 37
MES-2110(config-interface)# exit
MES-2110(config)# interface port-channel 2
MES-2110(config-interface)# vlan-stacking role access
MES-2110(config-interface)# vlan-stacking SPVID 48
MES-2110(config-interface)# exit
MES-2110(config)# interface port-channel 10
MES-2110(config-interface)# vlan-stacking role tunnel
MES-2110(config-interface)# exit
MES-2110(config)# vlan 24
MES-2110(config-vlan)# tagging 10
MES-2110(config-vlan)# untagging 1,2
MES-2110(config-vlan)# exit
MES-2110(config)# interface port-channel 1,2,8
MES-2110(config-interface)# frame-type fallback
MES-2110(config)# exit
MES-2110# show vlan stacking

VLAN Stacking:Enabled
SP TPID:0x9100
Port       Role       SPVID       Priority
-----------------------------------------
1          Access        37              0
2          Access        48              0
3          Normal         1              0
4          Normal         1              0
5          Normal         1              0
6          Normal         1              0
7          Normal         1              0
8          Normal         1              0
9          Normal         1              0
10         Tunnel         1              0
```

24

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- MES-2110 Access and Login
- MES-2110 Configuration and Console

24.1 Power, Hardware Connections, and LEDs

The MES-2110 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the MES-2110.
2. Make sure the power adaptor or cord is connected to the MES-2110 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the MES-2110.
4. If the problem continues, contact the vendor.

The **ALM** LED is on.

1. Disconnect and re-connect the power adaptor or cord to the MES-2110.
2. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 3.4 on page 35.
2. Check the hardware connections. See Section 24.1 on page 207.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor or cord to the MES-2110.
5. If the problem continues, contact the vendor.

24.2 MES-2110 Access and Login

I forgot the IP address for the MES-2110.

1. The default IP address is **192.168.1.1**.
2. Use the console port to log in to the MES-2110.
3. If this does not work, you have to reset the device to its factory defaults. See Section 5.6 on page 59.

I forgot the username and/or password.

1. The default username is **admin** and the default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 5.6 on page 59.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the MES-2110.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 3.4 on page 35.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the MES-2110. (If you know that there are routers between your computer and the MES-2110, skip this step.)

5 Reset the device to its factory defaults, and try to access the MES-2110 with the default IP address. See Section 5.6 on page 59.

6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

Try to access the MES-2110 using another service, such as Telnet or over the console port. If you can access the MES-2110, check the remote management settings to find out why the MES-2110 does not respond to HTTP.

Some possible reasons for being unable to connect over the in-band management ports are that you:

1 Deleted the management VLAN (default is VLAN 1).

2 Deleted all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the MES-2110.

3 Filtered all traffic to the CPU port.

4 Disabled all ports.

5 Misconfigured the text configuration file.

6 Prevented all services from accessing the MES-2110.

7 Changed a service port number but forget it.

See Chapter 23 on page 179 for details on managing the MES-2110 through the console port. This will allow you to correct any mistakes you may have made in the Web Configurator.

I can see the **Login** screen, but I cannot log in to the MES-2110.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.

Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.

3 Disconnect and re-connect the cord to the MES-2110.

4 If this does not work, you have to reset the device to its factory defaults. See Section 5.6 on page 59.

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

24.3 MES-2110 Configuration and Console

I'm trying to configure MVR but I get an error message.

MVR only functions with Tag-Based (802.1q) VLANs. To rectify this:

- Open the **Configuration > VLAN Menu > VLAN Type** screen and set the **VLAN Type** option to Tag-Based (802.1q).

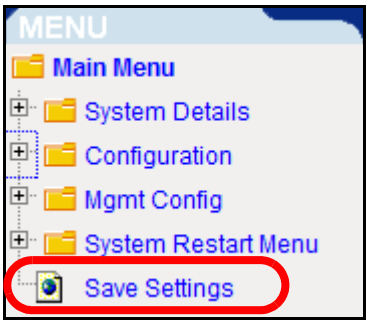
Or

- Connect to the MES-2110 through the console port (Chapter 23 on page 179) and enter the following commands:.

```
MES-2110: enable
MES-2110# configure terminal
MES-2110(config)# vlan-type 802.1q
```

I applied changes in the Web Configurator but they are not taking effect.

- Makes sure that you saved all configuration changes using the **Save Settings** link in the Web Configurator's navigation pane.



- Clean out the cache of the browser that you are using to connect to the MES-2110's Web Configurator, and make sure that you're only using a browser supported by the device (Chapter 1 on page 19)
- Try making your changes through the MES-2110's command line interface (Chapter 23 on page 179), and using the **write memory** command to make the changes permanent.
- Power off the MES-2110, then power it back on and make your changes afresh.
- Reset the MES-2110 to its factory default settings (Section 5.6 on page 59).
- If the problem continues, contact the vendor.

I cannot connect to the Web Configurator over the console port.

Ensure that your console settings are configured with the following settings:

SETTING	DEFAULT VALUE
Terminal Emulation	VT100
Baud Rate	9600
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

I keep getting 'Invalid command' messages when trying to configure the MES-2110 over the console port.

- There are a number of different modes in the MES-2110 command line interface. In order to use certain commands, you must be in the appropriate mode. See Chapter 23 on page 179 for information on the different modes, how they work, and which commands you may use in them.
- To see which commands are available to you while using the command line interface, type **?** and press **[ENTER]**.

I enabled ARP inspection on my MES-2110 but it doesn't seem to be working.

It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the MES-2110 has enough time to build the binding table.

My changes in the Web Configurator keep getting overwritten.

The MES-2110 allows up to five different accounts to access its Web Configurator. Make sure that you and another user are not modifying the device at the same time. Any changes you make will be overwritten when the other user saves his or her changes, and vice versa.

Every time I try to change the MES-2110's IP address over Telnet, I get an error.

You cannot change the device's IP address over Telnet.

25

Product Specifications

The following tables summarize the MES-2110's hardware and firmware features.

Table 84 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	268 mm (W) x 128 mm (D) x 44 mm (H)
Weight	1.2 kg
Power Specification	AC: 110-240V AC, 50/60 Hz, 14 W Max. DC: -36V~-56V DC, 14 W Max.
Interfaces	8 10/100 Base-Tx ports 2 GbE Dual Personality interfaces (Each interface has one 1000Base-T RJ-45 port and one Small Form-Factor Pluggable (SFP) slot, with one port active at a time.) 2 mini-GBIC (SFP) slots Auto-negotiation Auto-MDIX One console port Compliant with IEEE 802.3/3u Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x)
LEDs	Per switch: PWR, SYS Per Fast Ethernet RJ-45 10/100 port: LNK/ACT Per mini-GBIC slot: LNK, ACT Per mini-GBIC slot (in dual personality interface): LNK/ACT
Operating Environment	Temperature: 0º C ~ 50º C Humidity: 10 ~ 95% (non-condensing)
Storage Environment	Temperature: -40º C ~ 70º C Humidity: 10 ~ 95% (non-condensing)

Table 85 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234
Number of Login Accounts Configurable on the Switch	5 accounts configured on the MES-2110.
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
VLAN Stacking	Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address.
IGMP Snooping	The MES-2110 supports IGMP snooping, enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your MES-2110.
QoS	Queuing is used to help solve performance degradation when there is network congestion. The following scheduling services are supported: weighted round robin and all high before low queuing. This allows the MES-2110 to maintain separate queues for frames from each individual source or flow and prevent a source from monopolizing the bandwidth.
Bandwidth Control	Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.
Broadcast Storm Control	The device supports per port TCP/IP ingress rate limiting along with independent storm prevention.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.

Table 85 Firmware Specifications

FEATURE	DESCRIPTION
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
L2 Multicast	The device supports Layer-2 multicast switching with line-rate (wire speed) switching for all packet sizes and conditions. In addition, the MES-2110 can send packets to Ethernet devices that are not VLAN-aware by untagging (removing the VLAN tags) IP multicast packets.
STP (Spanning Tree Protocol)	STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a MES-2110 to interact with other STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.
Loop Detection	Use the loop detection feature to monitor any network loops on the edge of your network.
IP Source Guard	Use IP source guard to filter unauthorized DHCP and ARP packets in your network.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the MES-2110 allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the MES-2110.
Authentication and Accounting	The MES-2110 supports authentication and accounting services via RADIUS.
Device Management	Use the web configurator or commands to easily configure the rich range of features on the MES-2110.
Syslog	The MES-2110 can generate syslog messages for system monitoring.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or TFTP tool to put it on the MES-2110. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the MES-2110's configuration and put it back on the MES-2110 later if you decide you want to revert back to an earlier configuration.

The following list, which is not exhaustive, illustrates the standards supported in the MES-2110.

Table 86 Standards Supported

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 894	Ethernet II Encapsulation
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs
RFC 1757	RMON
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2138	RADIUS (Remote Authentication Dial In User Service)
RFC 2139	RADIUS Accounting
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 3046	DHCP Relay
RFC 4330	Simple Network Time Protocol(SNTP)
IEEE 802.1x	Port Based Network Access Control
IEEE 802.1D	MAC Bridges
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1Q	Tagged VLAN
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.3	Packet Format
IEEE 802.3ad	Link Aggregation
IEEE 802.3x	Flow Control
Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

A

Changing a Fuse

This appendix shows you how to remove and install fuses for the MES-2110.

If you use a fuse other than an included fuse, make sure it matches the fuse specifications in the appendix on product specifications.

Removing a Fuse

Disconnect all power from the MES-2110 before you begin this procedure.

1. Remove the power cord from the MES-2110.
2. See the product specifications for the location of the fuse. Use a small flat-head screwdriver to carefully pry out the fuse housing.
3. A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing. Pull gently, but firmly, to remove the burnt out fuse from the fuse housing. Dispose of the burnt-out fuse properly.

Installing a Fuse

1. The MES-2110 is shipped from the factory with one spare fuse included in a box-like section of the fuse housing. Push the middle part of the box-like section to access the spare fuse. Put another spare fuse in its place in order to always have one on hand.
2. Push the replacement fuse into the fuse housing until you hear a click.
3. Push the fuse housing back into the MES-2110 until you hear a click.
4. Plug the power cord back into the unit.

B

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 87 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.

Table 87 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 87 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

C

Legal Information

Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品, 在居住的環境使用時,
可能造成射頻干擾, 在這種情況下,
使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

A

abnormal traffic detection 175
accounts 172
alarms 170
application
  backbone 19
  bridging 20
  metropolitan 22
  trunking 21
  VLAN 21
ARP inspection 141, 147
auto negotiation 66

B

backbone application 19
bandwidth control 111
BPDU 90
bridge 89
  BPDU 90
  configuration 92
  path cost 89, 93
  port states 91
  priority 93
Bridge Protocol Data Unit, see BPDU
bridging application 20
broadcast 123
broadcast storm control 113

C

configuration
  bandwidth control 111
  bridge 89, 92
  broadcast storm control 113
  date/time 168
  DHCP snooping 143
  IGMP 125
  jumbo frames 75
  link aggregation 119
  loop detection 71
  MAC filtering 154
  multicast 125
  MVR 129
  port mirroring 115
  ports 65
  QoS 158
  trunking 119
  VLAN 99
configuration file 177
connection test 173
console port 30, 165
console port (accessing the CLI) 179

D

date/time 168
DHCP
  Option 82 137
  relay agent information 137
DHCP binding 145
DHCP client 62, 63
DHCP snooping 141, 142, 143
DoS 174
duplex 66

E

external authentication server 84

F

firmware upgrade 176
flow control 66

forward delay 93
forwarding frames 98
front panel 29

G

Gigabit Ethernet ports 30

H

hardware
  console port 30
  front panel 29
  Gigabit Ethernet ports 30
  installation 25
  LEDs 35
  mini-GBIC slots 31
hash mode 120
Hello Time 93
help (in the CLI) 180

I

IEEE 802.1x
  port authentication 77
IGMP 123
  configuration 125
  snooping 123
installing hardware 25
IP address 62
IP DSCP priority 161
IP source guard 141
  ARP inspection 147
  configuration 143
  DHCP snooping 142

J

jumbo frames 75

L

LEDs 35
link aggregation 117
  configuration 119
  dynamic 117
  hash mode 120
  ID 118
  static 118
  status 121
  system priority 121
lockout 59
login 51, 179
logout 181
logs 170
loop detection 71

M

MAC filtering 151
  configuration 154
  MAC learning 153
management 165
  abnormal traffic detection 175
  alarms 170
  configuration file 177
  connection test 173
  console port 30, 165
  date/time 168
  DoS 174
  firmware upgrade 176
  logs 170
  reset 178
  SNMP 166
  user accounts 172
  web configurator 51
management VLAN 109
max age 93
metropolitan application 22
mini-GBIC slots 31
multicast 123
  configuration 125, 129
  IGMP snooping 123
  MVR 127
Multicast VLAN Registration, see MVR

MVR 127
configuration 129

N

naming the system 62
navigation panel 54

P

password 58
path cost 89, 93
port authentication
and RADIUS 84
port configuration 65
port mirroring 115
port-based VLANs 99
power module
current rating 34
power wire 34
priority mode, QoS 159

Q

QoS 157
configuration 158
IP DSCP priority 161
port priority 160
priority mode 159
tag priority 161

R

RADIUS 84
advantages 84
and port authentication 84
server 84
Rapid Spanning Tree Protocol, see RSTP
reset 59, 178
RMON status 68
RSTP 89
BPDU 90
bridge priority 93
configuration 92
path cost 89, 93
port states 91

S

shortcuts 180
SNMP 166
SNTP 168
stacking, VLAN 105
stacking, VLANs 101
static bindings 141
status
IGMP 127
link aggregation 121
MAC filtering 152
multicast 127
ports 67
RMON 68
trunking 121
switch lockout 59
system
abnormal traffic detection 175
configuration file 177
connection test 173
DHCP client 62, 63
firmware upgrade 176
information 61
IP address 62
lockout 59
login 51
logs 170
name 62
password 58
reset 59, 178
user accounts 172

T

TACACS+ 84
Tag Protocol Identifier, see TPID

tag-based VLANs 107
tagged VLANs 97
time/date 168
TPID 103
trunking 117
  application 21
  configuration 119
  dynamic 117
  hash mode 120
  ID 118
  static 118
  status 121
  system priority 121

U

unicast 123
user accounts 172

V

VLAN 97
  application 21
  configuration 99
  forwarding frames 98
  frame formats 104
  management VLAN 109
  port-based 99
  stacking 101, 105
  tag format 103
  tag-based 107
  tagged 97

W

web configurator 51
  navigation panel 54
weighted round robin scheduling 157